An Analysis of Federal Policy on Internet Consumer Privacy and a Study of the Relationship between Privacy, Information, Trust, and Valuation

A THESIS
SUBMITTED TO THE FACULTY OF THE GRADUATE SCHOOL
OF THE UNIVERSITY OF MINNESOTA
BY

William P Bushey

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN SCIENCE, TECHNOLOGY, AND ENVIRONMENTAL POLICY

Steve Kelley

August 2011

Freedom is hammered out on the anvil of discussion, debate, and dissent.

-Hubert H. Humphrey

Abstract

Recent regulatory, judicial, and political action has reopened the question of how online consumer privacy from private organizations should be regulated in the United States. This paper analyzes the existing policy of the federal government (particularly of the Federal Trade Commission) regarding online privacy to determine if this policy has met its goals and the strengths of weaknesses of current policy. This paper also presents the execution and analysis of an empirical survey, motivated by the aforementioned policy analysis, to understand the relationships between privacy, the trust that individuals place in parties providing privacy assistance via privacy information aids, and the value that individuals place in privacy information aid provision. Results of this survey demonstrate that 1.) individuals are more trusting of third party providers of privacy information aids than first party or commercial website providers of privacy information aids; 2.) the trust that individuals have of a privacy information aid provider is not significantly impacted by the involvement of federal oversight; and 3.) individuals are unwilling to directly pay for privacy information aids. Finally, these analyses inform the discussion of three policy alternatives presented in an attempt to address the central policy question of this paper: are there actions that federal policymakers can take to promote the provision and use of privacy information aids?

Table of Contents

List of Tables

List of Figures

Abbreviations

DMA – Direct Marketing Association

DPD – Data Protection Directive

EU – European Union

FCC – Federal Communications Commission

FTC – Federal Trade Commission

FIPP – Fair Information Practice Principles

IITF – Information Infrastructure Task Force

OBA – Online Behavioral Advertising

OPA – Online Privacy Alliance

NAI – Network Advertising Initiative

NTIA – National Telecommunications and Information Administration

PII – Personally Identifiable Information

Chapter 1 - Introduction

For over a decade the policy of the United States federal government regarding the privacy of Internet users from commercial websites has been to encourage websites to describe their information collection, usage, and sharing practices to users in order for users to make informed decisions about their online habits. Unfortunately, those privacy disclosures that were meant to help individuals protect themselves have become incomprehensible blocks of text, a reflection of the increased complexity of website data practices and the online privacy environment. In response, a public discussion is underway among policymakers, industry, consumer groups, and activists to answer the question of how the federal government should act to protect consumer privacy online. The spectrum of proposed solutions spans from slight modifications of the current policy to implementation of strong government oversight and regulation. This analysis suggests that for the near future the discussion should focus on the modification side of the spectrum. Weaknesses of the current policy should be identified and addressed.

One identifiable weakness of current policy is its inability to provide individuals with the information they need to make informed decisions about online privacy. A potential remedy for this weakness is to provide individuals with content or computational tools that help them to understand the information needed to make informed decisions. These tools and content, which I will refer to as *information aids*, can include text-based summaries of privacy policies, labels that indicate the level of privacy protection that a website provides, or digital platforms such as P3P that allow software to act on a user's behalf to protect his or her privacy based on information that the website provides.

Developing these information aids is a tough problem for academics and engineers. Promoting their availability and use is a tough problem for policymakers. The latter problem informs the principal policy question of this thesis: are there actions that federal policymakers can take to promote the provision and use of privacy information aids? In an attempt to answer this question, this thesis employs an empirical study to address two sub-questions. First, the study examines the factors that impact one of the main determiners of an individual's decision to make use of a tool or piece of information – trust – to address the question of if and how federal policy can increase the trust that individuals have for privacy information aid providers. Second, this thesis considers a potential funding strategy for information aid providers by addressing the question of whether American Internet users are willing to pay directly for information aids.

The remainder of this thesis is structured as follows: Chapter 2 discusses what privacy is, analyzes the federal government's policy regarding individual online privacy, and argues for the modification of current policy to encourage information aid provision instead of the development of an entirely new policy. Chapter 3 reviews the literature related to trust, valuation, and online privacy, and defines the hypotheses regarding privacy, trust, and valuation that will be tested via a scientific study. Chapter 4 describes the methodology employed to execute a scientific survey, which used summaries of privacy policies as a proxy for information aids, and collected data about the trust and willingness to pay among the public for information aids. Chapter 5 presents an analysis of the collected data, the results of hypothesis tests, and the limitations of the study as performed for this thesis. Finally, Chapter 6 discusses the implications of the findings of the performed study for a policy of information aid provision, and describes three policy alternatives for consideration by policy makers.

Chapter 2 - Background

This chapter will provide background regarding online privacy and set the context in which this paper is written. First, this chapter will establish that individual online privacy protection from private organizations should be a matter of public policy discussion by demonstrating that there is a significant concern for privacy among the American public. Next, justifications for the protection of privacy, as well as the nature of privacy will be discussed. Following this will be an in-depth review of the federal government's current and historic policy regarding online privacy, followed by an analysis of the strengths and weaknesses of the current policy. Finally, the strengths and weaknesses of current policy will inform a discussion of the policy question that this thesis attempts to address.

Public Concern for Privacy

Since the World Wide Web first attracted widespread consumer and business interest in the mid 1990s, online users have been concerned about its privacy repercussions. For instance, a survey conducted in 1996 found that respondents strongly agreed with the idea that they value being able to visit websites anonymously (4.6 / 5), that they should have control over who gets their demographic information (4.4 / 5), and that they should be able to assume different aliases at different times online (3.7 / 5). The same survey also found that respondents disagreed with the idea that content providers have the right to resell information collected about users (1.7 / 5) (Pitkow and Kehoe, 1996).

As the Internet has continued to grow in function and daily presence, privacy concerns have persisted or grown. Comparing results from 2002 and 2008 surveys which measured respondents' ranking of privacy concerns and levels of concern, Anton found that in general levels of concern for online privacy had increased over that six year period. Respondents to the 2008 survey were more concerned about information transfer, information collection, and personalized advertising than respondents to the 2002 survey had been. Considering reasons for the increase in concern, Anton cited the growth of social networking sites and the increased publicity of data breaches that had occurred between 2002 and 2008 (Anton, Earp, and Young, 2010).

The teenage and young adult populations highlight the public's concern for privacy online. Not surprisingly, adults have been concerned about the privacy of their children, as shown by a Pew finding that 81% of surveyed parents feared that teenagers share too much information online (Lenhart, 2005). However, teenagers are not as oblivious to privacy as their parents fear, and they express their concerns via privacy protecting behaviors. Just two years later, another Pew study found that teenagers make decisions and take actions to protect their privacy. Pew found that two-thirds of surveyed teens limited who could view their social networking profiles through privacy controls provided by social networking websites. Furthermore, nearly half of those who did not limit access provided false information to protect their privacy (Lenhart and Madden, 2007). In addition, a pair of surveys conducted in 2009 and 2010 among college freshmen Facebook users found that 90% of responding users had changed the site's privacy settings at least once since first using the site, with 63% indicated that they had changed their privacy settings two or more times (boyd and Hargittai, 2010).

Persisting concern among Americans for online privacy has manifested itself in many other ways, including complaints to various levels of government. A recent press release by the Office of the Attorney General for the State of New York noted that complaints regarding the

Internet, including complaints regarding privacy, were the most common complaints received by the office in 2010 (Office of the New York State Attorney General, 2011). At the federal level, the Federal Trade Commission (FTC) received approximately 7,500 complaints regarding online privacy between 2004 and 2008 (Gomez, Pinnick, and Soltani, 2009). Furthermore, the FTC has received online privacy complaints related to several high profile Internet companies, including Facebook (Electronic Privacy Information Center, 2010) and Google (Federal Trade Commission, "In the Matter of Google, Inc.", 2011).

Justification and Nature of Privacy

Privacy is notoriously difficult to define. Reflecting this difficulty, privacy has been described as "a chameleon that shifts meaning depending on context" (Kang, 1998). Privacy, despite having several and often vague definitions (Solove, 2009), elicits high levels of concern, indicating that some justification(s) must exist for the concept. In defining what privacy means, at least in the context of this paper, it is helpful to first understand the justifications for privacy. Following this, we can work backwards to establish what concepts or abilities fit the discussed justifications, and what threats to those concepts or abilities may exist.

Justifications for privacy stem from humanity's nature as both an individual and a social creature, and reflect the need of a person to function and develop as both. One such justification is the necessity of privacy for the development of an individual as a self distinct from the community that he or she is a part of. Without privacy to shield an individual from the constant gaze and judgment of a community, an individual does not have the opportunity to develop thoughts, feelings, mindsets, or interests that differ from those of the larger community, at least not to the extent that the individual would be able to defend his or her distinct ideas against the judgment of the community (Post, 1989). Development of self via privacy is also a benefit for the community itself, as communities generally evolve via diversity. Thus, despite the desire of a community for information about individuals for purposes of law enforcement, enforcement of community morality, economic reputation, etc… communities often value privacy as a social norm (Post, 1989). This conflict between community desire for individual privacy and community desire for individual information informs a concept that will reappear later in this paper, that many aspects of privacy are defined by the community and are dependent on the community's competing desires for information and privacy (Post, 1989) (Solove, 2009).

Privacy is also justified as a requirement for the development of relationships between individuals. One aspect that defines a relationship between individuals is the depth of information that is shared between those individuals. Acquaintances generally do not share deep thoughts, feelings, or personal histories, especially if they are potentially embarrassing. Intimate relationships, by contrast, involve considerable sharing of information, and are often defined by the experiences, histories, interests, etc… that are shared between individuals. Without the privacy which allows individuals to share deep information without concern for that information being shared with the larger community, intimate relationships cannot form (Solove, 2009). A similar justification is that privacy provides individuals with control over who they have relationships with, as privacy allows an individual to control who has information about him or herself. Privacy thus allows an individual to control, to some extent, who is in a social relationship with the individual, and the level of intimacy of that relationship (Solove, 2009).

Security is the final justification of privacy that will be discussed here. Privacy can be used as a tool to enable the security of an individual or organization against intrusions, interferences, and unauthorized information access (Moor, 1997). As the broadest justification, security contributes somewhat to the development of self and development of relationships justifications, as the security from social forces afforded by privacy is a major component of privacy's contribution to the development of self and relationships. In addition, privacy as a tool of security allows privacy's justification to extend to virtually any circumstance in which security is valued. For instance, the desire for personal safety contributes to privacy's justification because privacy prevents those who may do physical harm from knowing where an individual is. The same can be said of financial safety, in which the privacy of financial information prevents theft by others. Furthermore, privacy as a tool of security also allows privacy to contribute to the autonomy that an individual enjoys, as privacy can prevent coercion via physical intrusion or by interventions in systematic processes and structures. Thus, the justification of privacy as a tool of security is even stronger amongst individuals and communities that value autonomy.

With justifications laid out, we can discuss the abilities or concepts that fit these justifications. United States common law has recognized a qualified right to privacy for over a century, dating back to Warren and Brandeis' seminal article, "The Right to Privacy". Warren and Brandeis described privacy as a "right to be left alone", meaning that an individual should be free of intrusion or observation in situations in which that individual has a reasonable expectation of privacy (Warren and Brandeis, 1890). Following decades of case law, four specific privacy torts emerged: intrusion into seclusion, public disclosure of private facts, false light, and appropriation (Prosser, 1960). Together, these common law torts provide individuals with a legal tool by which to seek redress for the violation of specific aspects that make up privacy as defined by the law: uninvited intrusion into a private space for information gathering; uninvited publication of private information; uninvited publicity that leaves a false sense of an individual; and uninvited, public use of one's image.

Basing privacy on the "reasonable expectation" test reminds us of the dynamically social character of privacy. The reasonable expectation test is a proxy for judging a situation against social norms by asking how an objective, "reasonable" (i.e. representative of the average/normal) member of the community would judge or classify a situation. As applied in the privacy torts, the reasonable expectation test allows privacy to evolve as the social norms of a community evolve.

Despite the flexibility available in common law privacy, there appear to be new aspects introduced by computing and the Internet that the privacy torts don't address. Computing and the Internet create gray areas of data privacy that do not map well onto the yes/no possibilities of the reasonable expectation test. For example, when considering the collection of data about an individual on an e-commerce website, the situation appears to fall within the intrusion into seclusion tort. The reasonable expectation question would ask: does the website visitor have a community defined right to be secluded from the data gathering of the website? The individual is visiting a site and using infrastructure that would either be considered public or the property of some other owner, so it would seem that the visitor has the same expectation of seclusion as he/she would have physically visiting a department store, which is little to none. Yet, as a practical matter, when an individual visits a store, he or she still has an expectation that only certain information, largely dealing with the visit itself and any resulting purchase, will be collected. Furthermore, assuming an individual does not draw attention to him or herself, and does not make a purchase, the nature of information gathering in a physical space means that the individual may be able to visit the store and leave with nobody realizing that the individual was ever in the store. A website can gather significantly more information about an individual than a department store can, with a speed and certainty that cannot yet be matched in physical spaces. Does the lack of an expectation of seclusion extend to all information that can be collected about an individual? The yes/no expectation of privacy test, when applied to seclusion, does not leave room for a consideration that seems paramount in the information age: in any given situation, can an individual have an expectation of privacy for some information and no expectation for other information?

Due to the intricate privacy questions raised by information technology that cannot be addressed by the common law privacy torts, a theory of privacy in the information age began to emerge based on a concept of individual control of information privacy. Alan Westin began developing the *control theory* of privacy in the late 1960s, paralleling the mass introduction of computing systems in businesses and organizations. Control theory defines privacy of information as the ability of an individual or institution to control who receives information about themselves and how it is used (Westin, 1967). What is considered to be 'control' or tools of control vary; Goodwin defined privacy control as control over an individual's environment and control over information dissemination (Goodwin, 1991), while Moor suggested that empowering individuals to create categories of allowed access for their information would provide the control needed for individuals to protect their privacy (Moor, 1997). The unifying concept is clear however – providing individuals with an ability to control access and use of their information is the primary means of protecting privacy in the information age.

While academics continue to debate the strengths and weaknesses of control theory (Solove, 2009), this conception of privacy has heavily influenced the federal policy on online privacy. Federal policy often considers how best to provide tools and information to individuals that will enhance the control individuals have over access and use of information about them. For this reason, privacy as discussed in this paper will refer to the control theory conception of privacy. Defining privacy in this manner also informs the primary metric for judgment of federal online privacy policy that will be employed: the ability of the policy to provide individuals with useful tools or information that empowers individuals to protect their online information privacy.

Past and Present Federal Privacy Policy: An Overview and Analysis

In the United States, individualism has had a strong influence on the discussion of policy regarding privacy (Westin, 1967), owing to America's nature and identity as the world's most individualistic society (Hofstede, 1991). Individualism plays a peculiar role in the privacy discussion; it both raises our desire to maintain our privacy (Cho, Rivera-Sánchez, and Lim, 2009) and lowers our trust in the ability of others to preserve our privacy for us. This is especially evident when looking at the discussion of the role of government in individual privacy, for the government is the very entity that has the most power to protect the privacy of individuals from corporations, but due to its size and power, it can also pose the greatest threat to individual privacy (Mendez and Mendez, 2010).

To some extent, United States federal policy regarding Internet privacy developed in reaction to the online privacy policies of other nations. Mendez and Mendez noted that the prevailing political rhetoric of privacy, especially in the middle and late 1990s, included a desire to prevent the intervention of European Union (EU) privacy regulation into the affairs of American businesses. In fact, privacy discussions in general, in both the US and the EU, have revolved around enabling development of online businesses. In the EU, the rhetoric of market development led to an argument for federal intervention – EU wide privacy regulation was described as beneficial to European businesses as operating under a single privacy regime would be considerably easier than the varying, nation by nation regulations that existed at the time. In the United States, the rhetoric of market development led to the opposite argument – federal regulation, from either the US or the EU, would be too restrictive and evolve too slowly to allow American businesses to develop in the quickly changing market of the Internet (Mendez and Mendez, 2010). In addition, views regarding the source of privacy problems also differed between the EU and US policy makers, with EU policy makers seeing privacy violation as resulting from the misuse of new technology by organizations, while US policy makers viewed privacy violations as evidence that individuals did not have the tools required to protect their own privacy online (Rose, 2006).

Not surprisingly, these different views on the impact of federal intervention led to significant differences in the policy regimes that developed in the EU and the US. In the early 1990s, the EU began a policy drafting process which resulted in the 1995 adoption of the Data Protection Directive (DPD). The DPD requires EU member nations to adopt legislation regulating the collection, use, and disclosure of personal information by private organizations and establish Data Protection Authorities to approve, monitor, and assist in enforcing privacy regulation. The DPD has been described as an example of *co-regulation*, a form of regulation in which the government and industry representatives both participate in the creation and/or enforcement of regulation (Hirsch, 2010). Other nations, including New Zealand (Rose, 2006) and Canada

(Personal Information Protection and Electronic Documents Act) (Cavoukian, 2011), have implemented privacy regimes involving the creation of commissions specifically for privacy and the regulation or co-regulation of consumer information. In contrast, the privacy regime in the United States, with a few exceptions, is based on a form of industry self-regulation – the creation and enforcement of privacy rules by industry groups (Rose, 2006) (Hirsch, 2010).

Self-Regulation of Internet Privacy

In 1997 the Clinton Administration published a framework which would guide the administration's policy on the Internet. *The Framework for Global Electronic Commerce* (Clinton and Gore, 1997) outlined five principles for general Internet governance:

- "The private sector should lead";
- "Governments should avoid undue restrictions on electronic commerce";
- "Where government involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce";
- "Governments should recognize the unique qualities of the Internet"; and
- "Electronic Commerce over the Internet should be facilitated on a global basis"

Suggestive of the non-intervention rhetoric common in Internet policy debates, the Framework elaborates on the need for a market-oriented, non-regulatory approach to Internet governance so that American industries could develop with the new technology. The Framework also discussed policy intentions specifically for privacy. Building on the work of the administration's Information Infrastructure Task Force (IITF), the Framework recommended a set of Privacy Principles based on two fundamental precepts of awareness and choice:

> *"Disclosure by data-gatherers is designed to stimulate market resolution of privacy concerns by empowering individuals to obtain relevant knowledge about why information is being collected, what the information will be used for, what*

steps will be taken to protect that information, the consequences of providing or withholding information, and any rights of redress that they may have. "

The Framework also proposed three values for guiding Internet privacy governance:

- Information Privacy – individuals should have a reasonable expectation of privacy online;
- Information Integrity – consumer information should not be improperly altered or destroyed; and
- Information Quality – consumer information should be correct, timely, and relevant.

By 1997, the FTC had emerged as the leading federal agency on the issue of Internet privacy, having already held stakeholder discussions and workshops starting in 1995. Matching the administration's self-regulatory spirit, the Commission began a policy of industry self-regulation for the issue of privacy online. In fact, promotion of self-regulation had been one of the goals of the Commission's workshops (Federal Trade Commission, 1998).

In order to guide the industry's self-regulatory efforts, the FTC published guidelines for what it considered to be a comprehensive self-regulatory program. While the FTC's guidelines place no legal obligations on industry organizations, the FTC is able to strongly promote adherence to its guidelines by threatening support for and implementation of stronger forms of regulation if the Commission observes that the guidelines are not being followed (Mendez and Mendez, 2010). Adherence can also be promoted by leveraging authority granted to the FTC by Section Five of the Federal Trade Communications Act, which will be discussed shortly. The core of these guidelines were, and still are, the Fair Information Practice Principles (FIPPs), which the Commission adopted from the Department of Health, Education and Welfare's 1973 report *Records, Computers and the Rights of Citizens* (Hoffman, 2010). These principles are:

- **Notice/Awareness** – Consumers should be given notice of an organization's data practices before any information is collected. This principle is recognized as the most fundamental of all the principles. To be effective, notice "should be clear and conspicuous … unavoidable and understandable".
- **Choice/Consent** – Consumers should have options as to how collected information may be used, especially with regard to secondary uses of collected information. Opt-in and opt-out are commonly associated with these principles.
- **Access/Participation** – An individual should have the ability to view information collected about him/herself and contest collected information on the basis of accuracy and completeness.
- **Integrity/Security** – Collectors of information should implement reasonable managerial and technical measures to ensure the accuracy and security of information concerning consumers.
- **Enforcement/Redress** – In a self-regulatory regime, industry should enforce the above four principles by mandating compliance to a code embodying these principles for membership to industry associations, perform external audits of organization data practices, and create certifications for entities that comply with industry codes. In order to allow for redress of grievances, organizations should have a mechanism by which consumers may have concerns addressed and be compensated for harms due to a violation of a self-regulatory code.

Since establishing its FIPPs based self-regulatory regime, the FTC has continued to review its policy and make changes when needed. The Commission has maintained a consistent dialog with industry and consumer stakeholders, especially since 2006, in order to learn how technology, business practices, and consumer needs have changed and to gauge how effective its current policy regime is (Federal Trade Commission, 2010).

A product of this dialog has been a new set of self-regulatory principles specifically for a new data collection and use – Online Behavioral Advertising (OBA). Viewed by the industry as a more targeted and efficient form of advertising, OBA relies on the collection of behavioral information about an individual, such as previously visited websites and search engine queries, to deliver advertisements that are relevant to an individual. The new principles, originally published in 2007 (Federal Trade Commission, 2007) and refined in 2009 (Federal Trade Commission, 2009), apply the FIPP specifically to data practices involved in OBA:

- **Transparency** – Similar to Notice/Awareness, consumers should be provided with a clear, concise, "consumer-friendly", and prominent notice of the organization's data practices as well as the options that consumers have to limit collection and sharing of information.
- **Reasonable Security, and Limited Data Retention** – Based on Integrity/Security, organizations should take reasonable steps, based on the sensitivity of data collected and the nature of the company, to secure data collected about consumers, and to retain data only for as long as is necessary to fulfill a legitimate business or law enforcement need.
- **Affirmative Express Consent for Material Changes to Existing Privacy** – Based on Notice/Awareness and Choice/Consent, if an organization wishes to use data in a manner materially different from what the organization stated when the information was collected, the organization should obtain an affirmative express consent for the new use.
- **Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising** – Similar to Choice/Consent, organizations should collect sensitive data for

behavioral advertising only after obtaining an affirmative express consent from the consumer.

These principles for online behavioral advertising do not include a principle of Access/Participation. Thus, the self-regulatory regime the FTC is currently endorsing for online behavioral advertising may not include a means by which consumers may view or contest data collected about them. However, it is unclear whether the FTC has intended for these new principles to replace the FIPP in the online behavioral advertising context, or to be considered in addition to the FIPP.

Industry Implementations of Self-Regulation

The Online Privacy Alliance (OPA), an industry group formed by leading computing companies including AOL, IBM, and Hewlett-Packard in the mid 1990s, was among the first groups to implement a program of self-regulation. The group's *Guidelines for Online Privacy Policies* required OPA members to provide users with notice about collection and use of information, allow users to opt-out of uses and contest data accuracy, and implement data security measures. Unfortunately, the OPA was unable to attract widespread membership or compliance and eventually disbanded. Furthermore, the OPA's guidelines did not include a process for enforcing the guidelines, nor did it place any restrictions on the type of information that could be collected or the uses it could be put to (Hirsch, 2010).

Following the failure of the OPA, another group, the Network Advertising Initiative (NAI), formed specifically to create a self-regulatory program of online advertisers. The NAI published its set of principles, *Self-Regulatory Principles for Online Preference Marketing by Network Advertisers*, in 2000. Like the OPA's guidelines, the NAI's principles required organizations to provide users with notice about collection of information. Unlike the OPA, the NAI distinguished between personally identifiable information (PII) and non-PII. PII refers to information that can specifically identify an individual on its own, such as a social security number, or can be easily combined with other information to identify an individual, such as a name combined with an address. Organizations were required to provide greater notice and consent if they collected PII. Notices had to include information about how PII would be used and distributed to third parties. PII collecting organizations were also required to allow users to opt-out of certain uses of PII. Also unlike the OPA, the NAI described a process of enforcement, indicating that a third party organization, TRUSTe, would enforce the principles via random audits of organizations, investigation of consumer complaints, revoking of NAI membership, and notification to the FTC and the public of significant violations. Like the OPA however, the NAI encountered difficulty attracting industry participation, with its membership dropping to as low as two in the mid 2000s (Hirsch, 2010). Furthermore, issues emerged regarding TRUSTe's enforcement, including questions about the effectiveness of the TRUSTe seal program on site privacy practices (Jensen and Potts, 2003) (Edelman, 2011), allegations that the organization never actually performed random audits, ending the practice of publically reporting complaints made about member companies by consumers, and the conflict of interest caused by TRUSTe's joining of the NAI. Following the failure of TRUSTe to enforce its principles, the NAI in 2008 revised its program and named itself the enforcer of its principles (Hirsch, 2010). As of May 2011, the NAI is still active, and its membership has grown to forty-two organizations under its self-enforcement policy (Network Advertising Initiative, "Participating Networks ", 2010). In addition to its self-regulatory program, the organization now also provides a tool for consumers to opt-out of participation in the behavioral advertising programs of its members (Network Advertising Initiative, “Opt Out of Behavioral Advertising”, 2010).

The Direct Marketing Association (DMA), an industry group with a history of self-regulatory programs for advertisers including the do-not-mail and do-not-call programs, entered into self-regulation of online behavioral advertisers in 2009 (Direct Marketing Association, “DMA Board Approves Guidelines”, 2009). In that year the DMA published a set of online advertising guidelines based on the DMA’s already existing Guidelines for Ethical Business Practice (Direct Marketing Association, 2010) and the Self-Regulatory Principles for Online Behavioral Advertising developed by itself and several other industry groups[1] (American Association of Advertising Agencies, 2009). As with the OPA and NAI’s guidelines, the DMA’s online advertising guidelines require that member companies provide notification via a privacy policy of information collection and practices, obtain consent for collection and use of certain sensitive information, and implement reasonable data security measures. The DMA’s online advertising guidelines also require member companies to provide clear notice of changes to privacy policies, encourages member companies to educate consumers about online advertising and privacy, and provides guidance on how notice and choice might be presented when advertisements appear on third party websites. Finally, the DMA provides for enforcement of its guidelines by an internal Corporate & Social Responsibility department and an Ethics Operating Committee, which hear cases concerning non-compliance of member organizations (Direct Marketing Association, “DMA Online Behavioral Advertising Alert & Guidelines”, 2009). Case proceedings are confidential and cooperation with the Committee regarding complaints is voluntary.

[1] Other groups involved include the American Association of Advertising Agencies (AAAA), the Association of National Advertisers (ANA), the Better Business Bureau (BBB), and the Interactive Advertising Bureau (IAB).

However, in the event that the organization does not cooperate with the Committee to address a complaint, the Committee may elect to publicize the case’s proceedings, censure the organization, and may suspend or expel the organization’s membership. If a complaint is received for a non-member organization, and that organization does not cooperate with the Committee, then the Committee may refer the case to federal or state law enforcement (Direct Marketing Association, 2011).

Exceptions to Self-Regulation

Self-regulation has been the federal government’s principal policy for Internet privacy. However, there are two significant exceptions to this policy: market or context specific legislation, and FTC enforcement of Section 5 of the Federal Trade Commission Act.

Congress has enacted legislation for the purpose of regulating privacy in a number of specific instances in which self-regulation was considered to be an inadequate policy. A number of acts, including the Privacy Act of 1974 (Ervin, 1974) and the Electronic Communications Privacy Act of 1986 (Kastenmeier, 1986), were enacted for the purpose of codifying and regulating the government’s ability to collect and use personal information about citizens via computer storage and telecommunications. At the urging of the FTC (Federal Trade Commission, 1998), Congress enacted the Children's Online Privacy Protection Act of 1998 (COPPA) (Bryan, 1998), which established a co-regulatory privacy regime for websites concerning their collection of information about Internet users under the age of thirteen. COPPA requires covered entities to provide a disclosure of their data practices, obtain parental consent before collecting information about users under the age of thirteen in a number of situations, and establish reasonable procedures to protect the security and integrity of information collected about users under the age of thirteen.

Specific markets have also seen privacy legislation enacted. The Health Insurance Portability and Accountability Act of 1996 (Kennedy and Kassebaum, 1996), a comprehensive act regarding health insurance practices, required the department of Health and Human Services to create and enforce a a privacy rule under Title II to regulate how covered entities may disclose the medical information of individuals, when consent of individuals and notice of uses is required, and requires entities to provide individuals with access to information about themselves and the ability to contest inaccuracies. Similarly, the Financial Services Modernization Act (Gramm, Leach, and Bliley, 1999), a comprehensive act regarding the management of financial service institutions, also created privacy regulations for financial institutions. Covered entities are required to provide notice to their customers about their data practices, customers' options for the sharing of their information, and any updates to the entity's practices. Entities must also implement managerial and technical programs for securing data collected about customers. In addition, entities must implement programs to protect customer information from attempts by others to access information via social engineering, a technique employed by some nefarious hackers to learn passwords and access procedures by manipulating or tricking individuals into revealing these facts.

Direct privacy enforcement has come about due to actions that the FTC has taken under its authority to enforce Section 5 of the Federal Trade Commission Act. Since the Internet began its commercial development in the mid 1990s, the FTC has used its Section 5 authority in actions related to online privacy in a number of cases, with all of these actions resulting in settlements between the FTC and the allegedly violating company that require specific actions that must be undertaken by the company (Hoffman, 2010).

The FTC does not have the authority to bring actions against companies that do not adhere to its guidelines, nor even specific authority regarding privacy except as granted by the above legislation. Instead, Section 5 allows the FTC to bring actions against companies that perform “unfair” or “deceptive” actions as described by the *FTC Policy on Unfairness* and the *FTC Policy Statement on Deception*. Unfair and deceptive actions cover a wide variety of activities that the FTC may investigate and punish, including a number of the most egregious violations of privacy (Hoffman, 2010).

When the FTC observes, or receives a complaint of, potentially unfair or deceptive actions, the Commission may initiate an investigation of the company in question. If, based on that investigation, the FTC finds that the company has engaged in unfair or deceptive actions, the Commission may decide to bring either an administrative enforcement action, in which the Commission brings a case before an administrative adjudicator, or a judicial action, in which the Commission files a suit in a federal district court. While a judicial action allows the FTC to pursue monetary damages and becomes effective immediately upon the court’s ruling, the FTC often pursues administrative adjudication since the administrative adjudicator will give significant deference to the FTC’s findings of facts and interpretations. However, to date all defendant companies have agreed to settle with the FTC (Hoffman, 2010).

As of 2011, the FTC has initiated actions against at least twenty companies for engaging in unfair or deceptive actions related to consumer privacy[2]. All of these cases have consisted of either a misrepresentation about security, a breach of a company's own privacy policy, or material changes to a company's privacy policy. All of these cases have also resulted in settlements between the companies and the FTC. While several of these settlements have aspects unique to the company involved, all include the common components of not allowing the company to misrepresent its data practices in the future; requiring the company to establish a comprehensive security program that is regularly audited by a third party; and requiring the company to keep records and submit reports to the FTC so that compliance with the settlement may be monitored (Hoffman, 2010).

Recently, the FTC brought a high profile action against Google regarding violations of privacy resulting from its introduction of Buzz (Federal Trade Commission, "In the Matter of Google Inc.", 2011). Google immediately settled with the FTC. Mirroring previous FTC privacy settlements, Google has agreed to display clear, plain English notifications of changes in its data practices and implement a privacy protection program across its organization, which includes the naming of individual(s) to oversee the program. In addition, this settlement requires Google to have third party privacy audits conducted annually for the next twenty years (Federal Trade Commission, "Google Inc, Agreement Containing Consent Order", 2011).

[2] Actions have been brought against ReverseAuction.com, Inc.; International Outsourcing Group, Inc.; ControlScan, Inc.; Guess?, Inc.; Tower MTS, Inc.; Petco Animal Supplies, Inc.; Guidance Software, Inc.; Life is good, Inc.; ValueClick, Inc (filed by Department of Justice in federal court on behalf of the FTC); Compgeeks.com & Genica Corporation; BJ's Wholesale Club, Inc; DSW, Inc.; CardSystems Solutions, Inc; TJX Companies, Inc.; Reed Elsevier, Inc.; Seisint, Inc.; Eli Lilly; Gateway Learning Corp (Hoffman, 2010); Twitter, Inc. (FTC, "In the Matter of Twitter, Inc., a corporation", 2011); and Google, Inc. (FTC, "In the Matter of Google Inc., a corporation", 2011).

Evaluation of Current Implementation

Notice/Awareness is the cornerstone of FTC, industry, and legislative policy on privacy. This is for good reason, as one of the principal reasons for concern over privacy online is the surreptitious nature of data collection possible on the Internet (Lessig, 2006, pg. 202-203) (Goodwin, 1991), which seriously undermines an individual's ability to control his or her privacy. In more than just rhetoric, notice/awareness has been the most active component of both federal and industry policy. Thus, it is worthwhile to evaluate the government and industry's success on this principle. Furthermore, the efficacy of this policy relies on the extent to which consumers read these notices and make use of the information provided in their decision making processes. Thus, it is worth reviewing the literature to understand the efficacy of relying on notice/awareness, and to discover how notice/awareness may be improved.

Rate of Notice Success

Figure 1 and Figure 2 display statistics gathered from studies conducted in 1998, 1999, 2000, and 2006 of the percentage of websites that displayed notices meant to inform visitors of the data practices of the website (Federal Trade Commission, 1998) (Culnan, 1999) (Culnan, 2000) (Federal Trade Commission, 2000) (Schwaig, 2006) (Williams, 2006). Each figure displays two trends lines, resulting from a distinction the FTC made between *information practice statements* and *privacy policies*. Information practice statements refer to statements made anywhere on a website that indicate, or allude to, any collection or use of information. Privacy policies refer to comprehensive passages describing all or a significant amount of the website's collection, use, and sharing practices. Together, the figures demonstrate that the percentage of websites providing notice of data practices to visitors increased significantly under the FTC's self-regulatory regime.

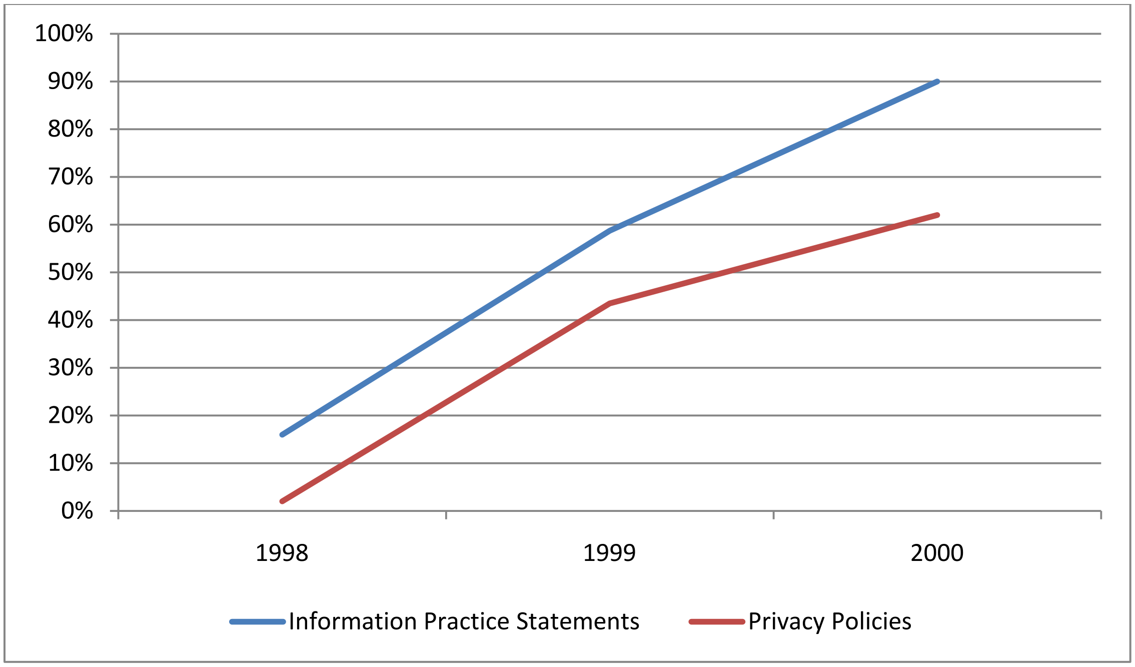


Figure 1 - Percentage of All Websites Displaying Information Practice Statements and Privacy Policies, by Year

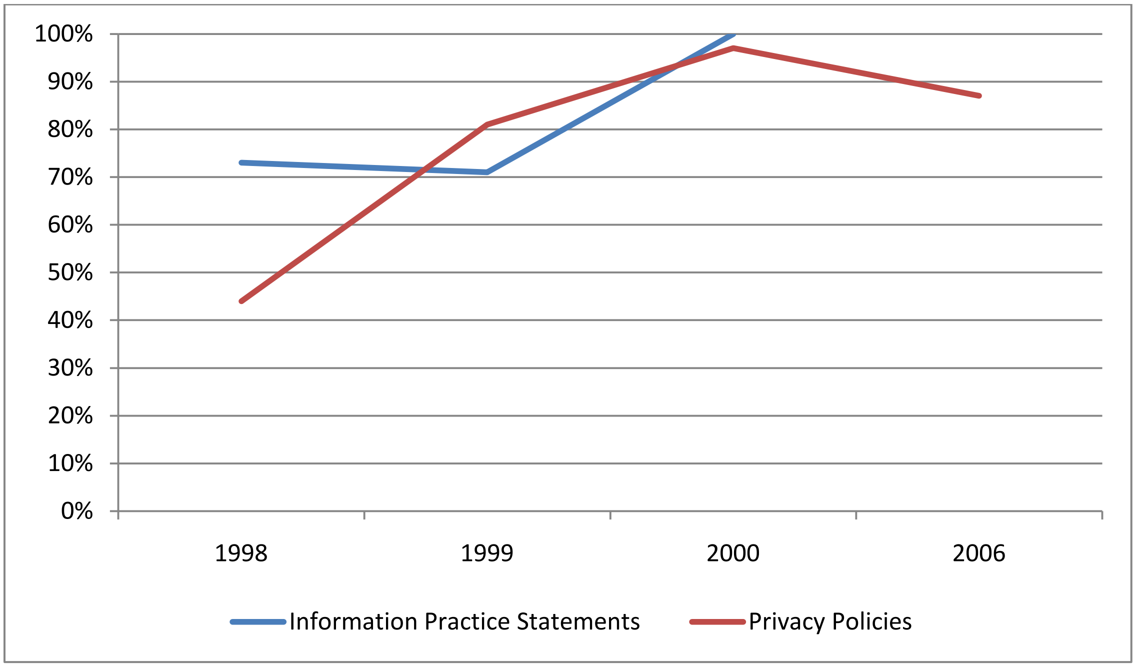


Figure 2 - Percentage of Popular/Fortune 500 Websites Displaying Information Practice Statements and Privacy Policies, by Year

As part of its 1998 report to Congress outlining a self-regulatory policy, the FTC also reported on the findings of a survey of the notice and data collection practices of 1,402 American websites, including 111 of the most popular at that time. At the time, a large majority of websites (approximately 90%) collected at least one form of consumer information. Despite this norm of data collection, very few websites displayed information practice statements or privacy policies, as indicated in Figure 1. Popular websites were significantly more likely to display a notice, as indicated in Figure 2, with approximately three quarters displaying at least one information practice statement and just under half posting a privacy policy. However, the data showed that significant gaps existed in the availability of notices online (Federal Trade Commission, 1998).

A set of studies performed by Georgetown (Culnan, 1999) (Culnan, 2000) and the FTC (Federal Trade Commission, 2000) in 1999 and 2000 followed up on the 1998 FTC study by tracking the change in percentage of websites that were notifying users of data practices. Like the 1998 FTC study, these follow up studies found that large majorities of websites were collecting personal information from users. As Figure 1 and Figure 2 indicate, the percentage of websites providing notice via information practice statements and privacy policies increased dramatically across all websites and popular websites. Privacy policies became nearly ubiquitous on popular websites by 2000, and a large majority of all websites were displaying some level of notice via information practice statements. A final pair of follow up studies focusing on the privacy policies of Fortune 500 websites showed that the practice of displaying privacy policies was still very common six years later. In fact, while the data showed that the percentage of Fortune 500 websites displaying privacy policies was a little lower than the percentage of popular websites in 2000, the percentage of websites of Fortune 500 companies with consumer facing or data focused businesses was about the same as the 2000 level for popular websites (Schwaig, 2006) (Williams, 2006).

Measured by the availability of notice of data practices online, the FTC's self-regulatory regime appears to be a success story for the federal government's policy for online privacy. Following two years of self-regulation, the practice of providing notice of data practices went from a rarity to an industry norm. Yet, to gauge its effectiveness, one must look at more than just the rate of notice presentation. Recalling the metric presented by the control theory of privacy, the success of a policy must be measured not only by the presence of tools that aid in privacy protection, but also by the usefulness of those tools.

Evaluation of Notices as Privacy Tools

A number of studies conducted in the early and mid 2000s showed that, in most situations, the majority of Americans do not read privacy policies despite their wide availability. In fact, one study found that only 3% of Americans regularly read privacy policies in general (Harris, 2001), while others found that only one quarter to one half will consult a privacy policy in situations in which knowledge of data practices and privacy is needed (Milne and Culnan, 2004) (Jensen, Potts, and Jensen, 2005). These low rates of usage significantly decrease the effectiveness of the federal notice/awareness based policy on privacy, and raise the question of why so few Americans make use of these provided privacy control tools.

A number of studies suggest seven primary reasons for the under utilization or under effectiveness of privacy policies as privacy control tools. One reason cited for consumers' lack of consulting website privacy policies is that many users misunderstand the purpose of privacy policies. Between half and three quarters of American users are under the mistaken impression that a website with a privacy policy will never share consumer information with other websites or companies (Turow, 2003) (Turow, Feldman, and Meltzer, 2005). As a result, users may feel that they do not need to read a website's privacy policy due to their belief that the website's practices are not threatening to their privacy.

Evidence suggests another, related reason for the underutilization of privacy policies by Internet users – privacy policies may not address the privacy concerns that Americans would like them to address. A 2005 study found that consumers ranked issues of sharing of collected data, notice of data collection practices, and storage of collected data as their first, second, and third greatest concerns. Yet only transfer was among the three most likely concerns to be addressed by privacy policies at the time, with notice and storage being the least likely to be addressed (Earp, et al., 2005).

The time and understanding required to read a privacy policy has been noted as a reason why Internet users do not read privacy policies. Researchers have observed that an Internet user may spend anywhere between four and twenty six minutes reading and understanding a privacy policy, depending on its length and the user's reason for reading the policy. The same researchers calculated that Americans would spend approximately half of their online time reading privacy policies, at an annual opportunity cost on the order of $3,534 per person ($781 billion nationally), if Americans were to read the privacy policy of every site they encounter the first time (McDonald and Cranor, 2008). As such, it is not surprising that 40% of American Internet users have stated that time is the primary reason they do not read privacy policies (Harris, 2001).

Complacency or malaise among experienced Internet users has also been offered as a reason for the lack of use of privacy policies by Internet users. A 2010 study found statistically significant evidence that those with greater levels of experience on the Internet are less likely to read privacy policies on websites. The same study also found evidence to support a hypothesis that a greater level of education will decrease the likelihood that an individual will read privacy policies (Beldad, de Jong, and Steehouder, 2010).

The most commonly discussed reason for Internet users' lack of utilization of privacy policies is that they are too difficult to understand. If users believe that they will not be able to comprehend a policy then they are less likely to attempt to read it (Milne and Culnan, 2004). As early as 2000, the FTC discussed the confusing nature of privacy policies, noting that the policies being posted by companies were often not consistent, did not clearly explain available choices to users, and were liable to change at any time (Federal Trade Commission, 2000). Formal analysis found that the average privacy policy requires the reading level of a college junior, and nearly a third require the reading level of a post-graduate. Only 1% to 6% are written at a high school reading level (Jensen and Potts, 2004) (Williams, 2006). These findings go a long way towards explaining why 29% of the 2001 Harris poll respondents indicated difficulty as a reason for their lack of reading privacy policies (Harris, 2001). These findings are also troubling in light of studies showing that Internet users with lower levels of education are more likely to attempt to read privacy policies than users with higher levels of education (Beldad, de Jong, and Steehouder, 2010) (Milne and Culnan, 2004).

In addition to the complexity of privacy policies, a knowledge gap among consumers is a reason for the under effectiveness of privacy policies as privacy control tools. For instance, a large majority of participants in a survey did not know that transfers of consumer information and information-based advertising are the economic norm of online content and service provision (Turow, 2003). Significant gaps and misunderstandings also exist among Americans regarding the actions and technologies available that can help or harm their privacy. Approximately half of American Internet users incorrectly believe that online merchants allow consumers to access or erase information collected about them and that websites do not share information with affiliates without consumers' permission (Turow, Feldman, and Meltzer, 2005). In an experimental setting it was found that a majority of users did not claim to be knowledgeable of P3P[3] or web-bugs, but did claim to be knowledgeable of cookies. Upon further investigation, even those who did claim knowledge of these technologies often could not demonstrate actual understanding of how these technologies impact their privacy (Jensen, Potts, and Jensen, 2005). It has also been found that majorities of American Internet users do not know how to obscure their IP addresses, compare privacy policies to their own privacy preferences, maintain anonymity online, secure emails, or describe privacy laws (Acquisti and Grossklags, 2004). Unfortunately, these gaps in information extend beyond the realm of Internet privacy, and include lack of information important for privacy protection in situations including mail-order commerce, supermarkets, charities, video rental, and a wide range of other consumer services (Culnan, 1995) (Turow, Feldman, and Meltzer, 2005) (Hoofnagle and King, 2008).

[3] P3P, Platform for Privacy Preferences, is a protocol proposed and developed in the early to mid 2000s by the World Wide Web Consortium (W3C) meant to create machine readable representations of site privacy policies and user privacy preferences in order for the creation of computing tools that assist users in understanding and managing the privacy environment they operate in.

The final stated reason for the underutilization and ineffectiveness of privacy policies is a sum of the previous six: the bounded rationality of Internet users. Developed in economics, bounded rationality is the concept that an individual may attempt to make a rational decision in some situation, but is limited by a number of constrained resources and cognitive abilities. Thus, the individual's rationality can be bounded by a lack of complete information, inaccuracies in available information, a lack of time to fully think about a decision and all of its relevant factors, an inability to recall or consider all relevant factors in decision, etc… In the case of privacy, bounded rationality plays a role in control of privacy because a lack of information and an inability to make use of provided information will limit an individual's ability to act in a manner that protects one's privacy. Beyond the issues described above, bounded rationality can also cause individuals to fail to consider seemingly obvious factors, such as the role of one's credit card institution in an online financial transaction (Acquisti and Grossklags, 2004).

Ineffectiveness of Current Self-Regulation

Beyond examining the success of privacy policies as the principal tool of privacy control, it is also important to consider how successful industry self-regulation is in relation to the other FIPP components: choice, access, integrity, and enforcement. The 1999 Georgetown surveys found that only 13.6% of all websites addressed all of the major components of the FIPP (Culnan, 2000), while only 20.4% of the most popular sites sample did the same (Culnan, 1999). By the time of the FTC's 2000 survey, 20% of sites from the survey's comprehensive sample were addressing all of the FIPP components, while 42% of the most popular sites were doing the same (Federal Trade Commission, 2000). Unfortunately, by 2006 only 4% of Fortune 500 companies that collected information had a privacy policy that addressed all of the FIPP components, according to one study (Schwaig, 2006). A similar study of Fortune 500 companies found that only 5.1% were considered "Fully Compliant" in 2006, and that 30.3% were considered "Compliant"[4] by the author (Williams, 2006). Unfortunately, while the practice of displaying privacy policies became a universal practice between 1998 and 2006, the quality of the data practices reflected by those policies decreased significantly, relative to the FTC's self-regulatory guidelines.

A 2009 study of the fifty most visited websites suggests considerable failures in adherence to the FIPP. An analysis of the privacy policies of the fifty most visited websites observed that 90% share information collected about users with "affiliates", which often include subsidiaries and corporate siblings, while 86% share collected information with third-party contractors. Yet these fifty websites do not provide a listing of affiliated companies or third party contractors, nor would they even provide a list when contacted by the researchers. This lack of notice is especially troubling when one considers the number of subsidiaries a company can have. For example, News Corp, owner of MySpace, has over 1500 corporate subsidiaries. It was also found that only 46% of websites granted any level of access to collected information by users in their privacy policies. Furthermore, 72% of privacy polices acknowledged that third-party, non-contracted, information collection occurs on their websites, but also state that the terms of the privacy policy do not apply to third-party collection. Often buried in the privacy policy and unread by consumers, this acknowledgement opens a considerable loophole in adherence to the consent principle, even on websites which are compliant to the principle for first party practices (Gomez, Pinnick, and Soltani, 2009). In addition, notice and consent of

[4] The differences between "Fully Compliant" and "Compliant" concerned the quality of compliance. Both categories represented companies that addressed all components of the FIPP, but "Fully Compliant" companies were considered to be more consistent in their compliance and were more likely to apply best practices in their compliance.

privacy policy changes are rarely executed, as noticed in a 2004 study which observed that only 19% of privacy policies described the intent of the company to actively notify users of policy changes, while 13% made no mention of how users would be notified of changes and 69% indicating that users would have to visit the privacy policy page to be notified of any changes (Jensen and Potts, 2004).

As described above, enforcement has been especially difficult to achieve under self-regulation. Prior attempts to implement self-regulation faced enforcement difficulties due to a lack of industry acceptance and the failure of independent bodies to follow through on enforcement responsibilities. Current self-regulatory enforcement lacks transparency. With the closed nature of the DMA's complaint process, a consumer lodging a complaint does not have the guarantee to fair and open adjudication that courts provide. Furthermore, the DMA's closed complaint process means that most consumers are unlikely to know if a given company is facing a challenge to its data practices.

The Policy Question

The above literature indicates that there are problems with the current execution of federal privacy policy, especially regarding the usefulness of the resulting privacy policies as tools for control of privacy. For its part, the FTC has long recognized a need for adjustments in its current policy, especially as it relates to notice and awareness. In 2006 then chairman Deborah Platt Majoras stated that:

> *"burying critical information in the End User License Agreement ("EULA") does not satisfy the requirement for clear and conspicuous disclosure. Buried disclosures do not work." (Majoras, 2006, pg. 7)*

Current chairman of the FTC and then commissioner Jon Leibowitz, has also voiced frustration with current privacy policies:

> *"Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies. They are often posted inconspicuously via a link at the very bottom of the site's homepage – and filled with fine-print legalese and technotalk." (Leibowitz, 2007, pg. 4)*

Recognition of a need for change extends to other federal agencies, including the National Telecommunications and Information Administration (Strickling, 2011) and the Department of Commerce (Department of Commerce, 2010).

In the face of evidence that the current policy may not effectively address the needs it was intended to, it is natural to consider whether there is merit to maintaining the current policy at all. If we were given a clean policy slate today, would we again create a light-touch, self-regulatory regime? Given the continued public concern for online privacy, and recent privacy violating events such as the Google Buzz introduction, it is tempting to wish for a more rigidly defined policy regarding what businesses can and cannot do with consumer information.

American individualism is still as prevalent today as it was in the 1990s. Given the history of individualism and the online privacy debate in the United States, this author questions the political feasibility of advocating for a policy regime of specific rules and strong government enforcement at this time. Attempts to introduce specific rules or strong government enforcement are likely to face the same firm calls for minimal government interaction that were prevalent in the 1990s and are likely to fail to gain the political support required for implementation. Furthermore, the self-regulatory regime has the significant advantage of flexibility, which I argue is still very much needed today.

Table 1 summarizes a number of technical and economic trends that are currently developing which raise privacy concerns. Each of the listed trends relies on collecting and using consumer information towards some end. As additional collection of personal information further reduces the control that individuals have about their personal information, each of these trends carries new treats to privacy. For example, location-based services create new threats to personal security due in part to their surreptitious information collection and wide distribution of personal physical information (Friedland and Sommer, 2010) (Blumberg and Eckersley, 2009), while smart grid deployment has raised public concern (May and Hull, 2011) because consumers see new and inexperienced collectors of information (Cavoukian, 2011) (Federal Energy Regulatory Commission, 2011) as yet another threat to their individual privacy.

Trend	Benefit
Online Personalization	Online services, such as search engines and social networking sites, can organize massive amounts of data to improve functionality and user experience based on information about the user (Smyth, 2007).
Location Based Services	A source of information for online personalization; allows online services to be targeted to individuals based on their physical location.
Cloud Computing	Centrally operated and managed computing resources are significantly more efficient in energy and costs than distributed personal computers. Also provide users with greater mobility, as services and data can be accessed from anywhere via the Internet (Horrigan, 2008) (Armburst, et al., 2009).
Smart Grid	Information about consumer energy demand and the state of the distribution network allow for more efficient production and delivery of electricity.
Advertising Driven Online Economy	Like many previous media (newspapers, television, radio), websites have not been able to establish a sustainable, subscription based model. Advertising, made more valuable by consumer information, is the chief source of revenue for many online service and content providers (Horan, 2011), including online journalists (Waldman, 2011, pg. 334 - 336).

Table 1 - Developing Trends with a Privacy Dimension

Regardless of one’s opinion regarding these trends, one must acknowledge that these trends are developing for justifiable reasons. In every case, one reason for the trend’s development is its utility in addressing some community need or desire. Online personalization, location-based services, and cloud computing serve to address the desire of consumers or organizations for improved usability and efficiency in the information technology that now permeates our society; a desire which one side may argue is merely a quest for mechanical improvements driven by an overreliance on technology while another side may argue is an economic necessity for the evolution of markets that can better provide the goods and services that consumers demand. The efficient energy production and distribution that can be made possible by a smart grid can address, in part, the various economic, scientific, and political demands placed on our nation’s energy policy. Finally, as media and journalism continue their migration to the Internet, consumers and businesses alike demand an economic model to fund online content and services as cheaply and conveniently as possible. As an evolution of the traditional advertising-based models of previous media, online advertising appears to address this demand, and is currently the economic engine that powers the free speech and political watchdog functions of today’s online media and journalistic content providers.

Returning to the socially-dynamic nature of privacy, our society is in a period of reevaluation of privacy. American society is struggling with the question of how to merge the desire for privacy with other desires that are now achievable thanks to developing information technology. In the case of the desire for increased efficiency in information technology, our society has yet to even answer the question of whether the desire rises to the level of a societal need or value. The struggle to define and rank values can be seen in the back and forth of statements made by industry representatives, who see greater value in the efficiency their services provide and infer that their consumers feel the same way (Sprenger, 1999) (Arrington, 2010), and activists who counter that the social value of privacy has never been greater than it is today (boyd, 2010). Such a values based problem, with many developing and moving variables, requires a flexibility of policy similar to the flexibility of the reasonable expectation test of common law, so that the definition of privacy can evolve as social values become more defined. Thus, I contend that a light regulatory approach, at least with regard to rule definition, should continue so that our society can develop privacy rules over time, instead of seeking to install federal rules and laws regarding privacy that may not yet be mature.

That said, the current implementation of policy clearly fails to meet certain goals. A policy which leaves the establishment of values up to a distributed decision making process must provide roughly equal power among the participating parties to express their view on the value definitions and rankings. However, in the case of the current implementation of privacy regulation, one party, Internet users and consumers, has considerably less power to express its views than does another party, the operators of websites. As already discussed, bounded rationality limits the ability of an individual to consider complex decisions and sources of information, and thus their ability to form and express a decision. As organizations (in some cases exceedingly large organizations), the operators of websites do not suffer from bounded rationality to the same degree as individuals – organizations can dedicate resources to the tasks of complex decision making and expression. The related phenomenon of information asymmetry is also at play. Website-operating organizations are considerably more knowledgeable about data practices and the potential consequences of information collection, use, and distribution than are individuals. As a result, organizations have a greater capacity to make decisions and expressions regarding data practices and privacy than do individuals.

Combined, the current environment of individual bounded rationality and information asymmetry lend a considerable advantage to organizations' ability to influence the value definition and ranking process.

It follows that today's policy of privacy questions should focus on how government can best act to address the bounded rationality and information asymmetry problems of the current policy implementation. Unfortunately, these problems are very difficult. Some research has already sought to develop methods for conveying the meaning of online privacy policies (Vail, Earp, and Anton, 2008) and similar legal texts (Masson and Waldron, 1994). Such research endeavors have yielded measurable successes, but also demonstrate that further research and development must occur in the realm of information aids for privacy policies that can address bounded rationality and information asymmetry. As problems still in need of technical and scientific solutions, federal policy needs to focus on how to support and guide the research and development of solutions to these problems.

In December of 2010 the FTC released a comprehensive report commenting on the current policy implementation concerning online consumer privacy. The report also outlined future policy goals which suggest that the FTC seeks to address the bounded rationality and information asymmetry problems of current policy. Of its three broad goals – industry implementation of Privacy By Design, creation of simpler and more streamlined privacy choice mechanisms, and increased transparency of business data practices – two speak directly to the bounded rationality and information asymmetry problems. Recognizing the breadth of the problem at hand, the report also presented dozens of questions to industry and academia, intending to prompt research and comments regarding how best to convey information to individuals about data practices and provide choice mechanisms that individuals will be able to understand and use (Federal Trade Commission, 2010).

The questions and analysis presented in the FTC's 2010 report focus on how portions of the bounded rationality and information asymmetry problems should be addressed. The report does not explicitly discuss the question of who should be the primary party to address these problems. Instead, the report assumes that industry groups and website operators should be primarily responsible for addressing the bounded rationality and information asymmetry problems found in online privacy today. As evident by Facebook's recent launch of its new description of its privacy policy (Facebook, 2011), and activity regarding the Do Not Track header (Zeigler, 2011) (Wingfield and Angwin, 2011) (Albanesius, 2011) (Mozilla, 2011), industry seems to be hearing the FTC's message and is acting quickly to meet the Commission's suggestions.

The question of who should be the primary assistor of individuals regarding online privacy is worthy of further consideration. There are significant consequences to the decision (either implicit or explicit) of who should assume a role. Chief among these consequences is the provision of resources. Even if a policy does not discuss allocation of resources, the assumption that a party will be responsible for a task will lead to resources being allocated to that party by some entity, be it government, a private organization, or the market system. Another consequence is the implicit trust the government places in the chosen party's ability to perform the task in question.

As will be discussed in the next chapter, website operators may have natural motives that conflict with their ability to accurately and fully provide assistance to individuals regarding online privacy. Furthermore, previously discussed literature suggests a less than successful history of privacy assistance provision by website operators. These factors lead the author to question whether a policy that assumes website operators will be able to provide privacy assistance to individuals will prove to be the most efficient allocation of resources and government trust. If the assumed parties are not the most capable parties to address the problems at hand, than allocating resources to them to address the problems will lead to waste and a less than optimal solution.

This inefficient allocation of resources may be exacerbated by the issue of trust from both the government and individuals. Based on history and an understanding that website operators may be acting against their greater motives, individuals may not trust the aid that website operators attempt to provide them, and thus not make use of the provided aid. Such a scenario would further contribute to the inefficient allocation of resources. Such a scenario would also undermine the government's ability to effectively execute policy of any type in the future via its trust, including future policies on privacy, as this scenario would cause individual's to question the government's ability to properly assess the trustworthiness of parties.

The balance of this paper will seek to explore the relationship between online privacy and trust in an effort to inform the policy question of who the federal government should encourage to assist individuals regarding online privacy. The following chapter will establish via literature that consumers value less the services of organizations that they do not trust, and that trust is an important consideration of consumers when dealing with privacy in any form. Having established that assistance or information from an organization that consumers do not trust are unlikely to be used, this paper will then attempt to determine via a scientific study which factors influence the trust individuals place in parties regarding online privacy. Finally, the results of this scientific study will inform a discussion on the question of which type of party is best positioned to assist individuals to understand data practices and online privacy, and the potential actions that the federal government can take to maximize the ability of its current policy to provide individuals with tools that enable their control of their own personal information.

Chapter 3 - Trust and Contingent Valuation

Guided by the analysis and discussion of the previous chapter, this chapter presents the relevant scientific literature that will inform the scientific study performed for this thesis. First, a definition of trust and its measurable components will be provided. Then, a review of literature will be presented regarding the known relationships between trust, privacy, and willingness to pay, as well as the relationship between third parties and trust, and government and trust. Throughout the literature review, hypotheses will be posited, to be tested in the following chapters, about the relationships between trust, privacy, government involvement, first or third party involvement, and valuation in the context of provision of privacy information aids to individuals.

What Is Trust and How Is It Measured?

As this paper concerns the decisions of individuals to make use of aids provided by others, the *decision trust* definition will define the concept of trust as used in this paper. Decision trust, as defined by Jøsang, Ismail, and Boyd, is "the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible". This definition presents trust as a requirement for decisions in the face of a perceived risk that the dependee will fail in some capacity to perform an action depended upon. Considered another way, trust as defined here impacts the relationship between an individual's risk perception – the perceived likelihood that the dependee will fail to perform an action – and risk tolerance – the amount of perceived risk an individual is willing to accept when depending on another. If perceived risk is higher than risk tolerance, then an individual will likely decide not to depend on another party. If perceived risk is lower than risk tolerance, then the individual may decide to depend on the other party. Within this risk-based decision system, trust can act to reduce the risk an individual perceives by establishing that the dependee is reliable and that its actions carry a high utility.

Decision trust provides a concept of trust, but not a method for measuring it. For this, I turn to Mayer, Davis, and Schoorman's three measurable factors of trust: ability, benevolence, and integrity. *Ability* refers to the level of skill and competency that a party has to exercise influence in a specific situation or environment. *Benevolence* is the extent to which a dependee is motivated to be helpful or do good to the trusting dependent party. *Integrity* is the extent to which the dependee adheres to a set of principles, and the acceptability of those principles to the dependent (Mayer, Davis, and Schoorman, 1995). The impact of all three of these on the trust of an individual for another party are dependent on the individual's perception – the level to which the individual believes that the other party possess ability, benevolence, and integrity. Thus, measuring the level of trust that an individual has for another party involves measuring the level to which an individual perceives that another party exhibits these three factors.

Such measurements have been the basis for several studies that have examined the trust that individuals place in others. For this reason, ability, benevolence, and integrity will also serve as the basis for how trust will be measured in this paper. It is worth noting, that ability, benevolence, and integrity are measures relevant to the risk perceived by an individual, as they are measures of the reliability and utility that an individual perceives. However, these components do not provide a measure of the risk tolerance of an individual.

Relationship between Privacy Concerns and Trust

Given a definition of trust and a measurement for it, I now turn to the relationship between privacy and trust. A common theme in the literature on privacy is the impact that levels of concern have on individual behaviors and perceptions. For example, over the course of a decade and a half, Alan Westin conducted a number of surveys on privacy concerns and regularly categorized survey participants into one of three sets: *privacy fundamentalists*; *privacy pragmatists*; and the *unconcerned*. According to Westin, privacy fundamentalists are in general less trusting of organizations that ask for personal information, more worried about the accuracy and uses of collected data, and were more likely to employ privacy protecting practices and behaviors than the general public. Privacy pragmatists believe that trust can and must be earned by organizations wishing to collect data, will weigh the benefits that result from sharing their data against the potential risk of privacy violations, and will seek out practical tools or procedures that are available for the protection of privacy. The unconcerned are generally trusting of data collecting organizations and are willing to disclose personal information in exchange for goods or services. While aspects of this categorization are debated by academics (Kumaraguru and Cranor 2005), including the actual behaviors that group members exhibit and the populations of these groups, Westin's categorization of individuals via privacy concerns represents a useful concept. Privacy concerns of individuals vary and the actions that individuals take involving their personal data will depend in some way on their level of concern for privacy (Kumaraguru and Cranor 2005).

Statistical evidence exists to support a link between trust, privacy concerns, and privacy behavior. Based on a survey regarding willingness to share personal data based on the data practices of a website, Culnan and Armstrong found that in situations in which trust was not established between an individual and an organization those individuals with high levels of privacy concern would be less willing to disclose personal information for advertising. Culnan and Armstrong also found that in situations in which trust had been established via the display of fair information practices, an individual's level of privacy concern would not impact the individual's willingness to disclose personal information. Thus, trust as a result of an organization's data practices can overcome an individual's general concern for privacy and impact an individual's likelihood of providing personal information (Culnan and Armstrong, 1999). When considered within the decision trust framework, these findings suggest that fair data practices can reduce perceived risk by increasing the benevolence and integrity that individuals see in an organization, and that privacy concern may lower risk tolerance among individuals.

Analysis of a 1998 survey on privacy concerns and behaviors further confirms the link between privacy concerns and likelihood of disclosing personal information. The analysis also found that individuals with higher levels of privacy concern were more likely to require that organizations adhere to certain data practices before being willing to disclose personal data, thus demonstrating requirements for the benevolence and integrity components of trust described above. In addition, the analysis found that individuals who wished to have a privacy policy available are also more likely to require that an organization demonstrate trustworthiness before sharing data (Awad, 2006). Liu, Marchewka, and Ku also hypothesized and experimentally supported the positive influence that building trust via adherence to privacy protective data practices has on the intention of individuals to disclose information to a website (Liu, Marchewka, and Ku, 2004).

These and other findings on the relationship between trust, privacy concern, and data behaviors have contributed to the literature regarding *privacy calculus*. In essence a utility maximization model, privacy calculus posits that when individuals face a decision to undertake a potentially privacy violating activity, they will (either consciously or subconsciously) compare the perceived benefits they expect to receive from undertaking the action against the perceived risks of privacy violation. If the former is judged to be greater than the later then the action will be undertaken, otherwise the action will not be undertaken (Awad, 2006).

Much like its relationship with perceived risk within the decision trust concept, within privacy calculus trust is conceptualized as a social and psychological force that reduces perceived risk. In addition, within privacy calculus, trust can also be negatively influenced by perceived risk. A user's perception of a high risk of privacy violation by an organization will reduce that user's trust in that organization. However, other factors that positively influence trust by establishing ability, benevolence, and integrity, such as the display of certifications or information from an individual's friends and family about the organization, can increase trust enough within an individual so as to reduce the individual's perceived risk. This relationship between trust and perceived privacy risk was supported by a 2006 study, which found statistically significant negative influences on trust and willingness to provide personal information from perceived risk. A positive influence on willingness to provide personal information from trust was also found, as well as a positive influence on privacy concern from perceived risk (i.e. greater perceived risk led to higher levels of concern regarding privacy) (Dinev, 2006).

Of course, trust does not only impact the intentions or behaviors of individuals regarding privacy and data practices; trust impacts the behaviors of individuals in nearly all situations in which risk and dependence on another are present. Schlosser, et al., found that feelings of trust had a statistically significant influence on the likelihood that online shoppers would undertake shopping activities. Across multiple studies conducted by the researchers, feelings of trust in ability were found to influence intentions to purchase items from a given vendor, and feelings of trust in the benevolence of a site were found to influence the intentions of participants to browse a given vendor's site (Schlosser, White, and Lloyd, 2006).

A 2004 Milne and Culnan study of particular relevance to this paper establishes links between privacy concerns, trust, and tendency to read privacy policies. Based on a random sample of 2,468 U.S. adults, the researchers found individuals who trusted a given privacy policy to accurately represent a website's data practices were more likely to actually read that privacy policy. The same study also found support for the seemingly contradictory correlations that an individual's level of privacy concern would positively influence her likelihood of reading a privacy policy and negatively influence her trust in a privacy policy (Milne and Culnan, 2004).

Finally, a salient example of the impact of decision trust on general behavior is a study which found support for the notion that trust would influence the likelihood that individuals would either interact with a website or make use of its advice. Based on literature, the researchers posited that trust would impact an individual's intention to depend on, interact with, or accept information from a given party, and used these intentions as a proxy for the undertaking of trust-based behaviors. A framework was constructed and tested upon this premise, with testing occurring via a survey in which trust was measured for a situation most relevant to the guidance of the policy alternative discussed in the previous chapter: a website providing legal information and advice to participants. Results from this survey confirmed that feelings of trust do significantly impact the intentions of individuals to undertake actions in the experimental situation (McKnight, Choudhury, and Kacmar, 2002).

Taken together, the established relationships between privacy concern and trust in the context of data usage, and trust and use of a service in the general context, raise a question: what is the relationship between an individual’s concern for privacy and her trust of parties who attempt to provide privacy aid? Aside from being of interest to the privacy and trust literature, this question is also an important consideration for policymakers. Awad has suggested to decision makers in industry that it may not be a wise investment to meet the demands of those with higher levels of privacy concern (Awad, 2006). However, policymakers, in particular Congress and the FTC, face greater concerns than just the efficient use of a single organization’s resources. A group of individuals with high privacy concerns may form a highly visible and politically influential stakeholder group who must be satisfied in order for a policy to move forward. In addition, given the current need for discussion of the value of privacy, Congress and the FTC also need to provide a forum for this discussion, in addition to overseeing an efficient use of national resources.

In an attempt to answer the above question, the established relationship between privacy concerns and trust in the context of data actions will be extended to the context of a party attempting to aid an individual regarding privacy by providing a summary of a privacy policy. This would imply that individuals with high privacy concerns will, initially, have lower levels of trust in parties who provide privacy information aids, assuming no prior history between the two. Thus, the following hypothesis is proposed:

> *H1: An individual with a high level of concern for privacy will have a low level of trust for parties that provide privacy information aids.*

Who Is Trusted?

The literature informing the above hypothesis, along with the history of self regulation efforts discussed in the previous chapter, raise another set of questions. In the context of assisting individuals in understanding their privacy environment, is there a difference in the trust placed in a first party – such as an e-commerce website – and a third party – such as an organization whose focus is consumer privacy protection? As with the previous question concerning the relationship between privacy concern and trust, this question also is of interest to policy makers. As shown by previous literature, a policy that results in assistance offered by parties which are less likely to be trusted and thus less likely to be considered may be an ineffective policy. In considering the alternatives available to policy makers regarding trust and assisting individuals regarding privacy, the question also arises as to the impact that government actions can have on trust. Can an assurance from the government about the validity of a party's attempts to assist users regarding privacy positively impact the trust that individuals have for these assisting parties?

Trustworthiness Across Institutional Categories

Before examining the literature regarding trust of first vs. third parties, and government oversight, it is worth considering the trustworthiness of certain categories of third parties. Across the primary institutional categories of academic, private, non-profit, and government, the available literature presents a murky picture. For example, Turow found small or statistically insignificant differences in participants’ trust/distrust in the privacy activities of several institutions, including major advertisers, Microsoft, the government, banks and credit card companies, Internet service providers, and makers of privacy protection software. Turow also prompted respondents with questions regarding which institution they trusted the most to help them protect their online privacy and which institution they most expected to make an unauthorized disclosure of their privacy information. Representing the lack of difference in trust and distrust among institutions, between one quarter and one third of participants responded with the same institution to both of these questions (Turow, 2007).

An examination of available studies of trust based on sectors showed inconclusive levels of trust among the public for private, non-profit, academic, and government organizations. O’Neill examined trends from surveys conducted by Independent Sector, the Brookings Institute, and the University of Chicago’s General Social Survey. General trends among the surveys examined are that the academic organizations (public and private higher education institutions) cluster among the most trusted organizations; government organizations (federal, state, and local) cluster among the least trusted organizations; there is a sharp contrast within the private sector with small businesses appearing near the top of trusted organizations and major corporations appearing near the bottom; and trust in nonprofits varies widely depending on the type of nonprofit. Thus, certain types of organizations (academia and government) appear to elicit distinct, narrow ranges of trust, while others elicit a wider, non-distinctive range of trust. Category wide conclusions regarding private and non-profit firms can not be reached, as trust for these organizations depends on the subcategory that a given organization falls into. However, the evidence presented does suggest that academic organizations maybe the most trusted type of organization (O’Neill, 2009). Based on this suggestion, the remainder of the paper shall consider academic institutions when discussing a third party organization.

First vs. Third Party Trust

As discussed in the previous chapter, first parties, namely websites providing consumers with goods or services, have been successful in providing privacy assistance by providing privacy policies. Several surveys have shown that the existence of privacy policies and other notices on a website generally raise the level of trust an individual feels for that website (Turow, 2003) (Turow, Feldman, and Meltzer, 2005) (Beldad, de Jong, and Steehouder, 2010). While these studies focused on trust regarding preservation of privacy, it can be inferred from these studies that the positive impact that privacy notices have on trust regarding preservation of privacy includes an assumed trust in the first party to provide an accurate notice that assists individuals in understanding their privacy on the first party website. To the extent that individuals use the existence of privacy policies as a tool for evaluating the benevolence, integrity, and competence of websites regarding privacy, distrust in the privacy policies themselves would reduce the likelihood that individuals would use them as a tool of evaluation. Furthermore, distrust in the privacy policies may contribute to general distrust of the website regarding other services, as distrust in the privacy policies may lead an individual to question the general benevolence, integrity, and/or competence of the website.

Contributions among the various trust contexts can work both ways. A lack of general trust or a general distrust of a first party may negatively contribute to an individual’s trust of a website to provide privacy assistive services. In light of news coverage which likely reduces the level of trust among the population for certain high profile websites regarding privacy (Anton, Earp, and Young, 2010) (Federal Trade Commission, “In the Matter of Google, Inc.”, 2011) (Raphael, 2009), one might expect that the ability of these websites to build trust regarding its efforts to assist users in privacy to be hindered. Furthermore, less known or completely unknown parties traditionally also face difficulty establishing trust, and while these parties may attempt to build trust by providing guarantees or support opportunities, third parties often play a major role in influencing the trust that an individual may have for an unknown website (Jøsang, Ismail, and Boyd, 2007).

Beyond the trust interactions that may exist, there is a more fundamental reason that individuals may not trust first parties in attempts to aid individuals regarding privacy. Aids and tools are provided to individuals not only to protect individual privacy, but also to hold organizations accountable to laws and social norms. A conflict of interest is innate in a first party’s provision of a privacy information aid. An individual user is dependent on some information from the website regarding both the privacy that the individual should expect from the website and the accountability of the website to industry privacy guidelines. However, as a method of first party accountability, there are incentives for the website to not provide the aid to the fullest of its ability or with total accuracy[5] (Swift, 2001). Thus, individuals may have cause to be distrustful of websites providing their own privacy information aids.

This notion that users may trust the information provided by a third party is supported to some extent by several studies. A quantitative and qualitative study regarding trust of website content found that study participants often considered whether other websites linked to a given website or how search engines ranked a given website when determining the

[5] In the case of privacy policies, these incentives are marginalized to some extent by the quasi-legal/industry requirement that websites provide privacy policies, and the contractual nature of privacy policies as viewed by the FTC.

trustworthiness of the website's content, suggesting the role of validation by third parties (Hargittai, et al., 2010). In analyzing the privacy-related factors that influenced a survey participant's decision to make a purchase from a website, certifying marks from a third party (TRUSTe) were found to be the most influential factor among all factors tested, which included various types of privacy policies and contact information. Across models for specific populations and relationships, the third party mark was also found to be the most or among the most influential factors for participants deciding to make a purchase from a website (Jensen, Potts, and Jensen 2005). A similar study by Rifon also found that the presence of a privacy seal from a third party (either TRUSTe or BBBOnline) had a significant, positive impact on the trust an individual perceived in a website (Rifon, LaRose, and Choi, 2005).

Given the above, the following hypothesis is proposed regarding the question of whether individuals are more likely to trust privacy information aids from first party websites or from third party organizations:

> *H2: Users are statistically more likely to trust a privacy information aid created by a third party organization than one created by a first party.*

Trust in Government Oversight

Literature presents a largely negative view of trust among individuals for government. As stated above, government is generally the least trusted type of institution among the various institutional categories (O'Neill, 2009). Surveys of literature regarding both American and international trust in government show that in general, individuals are less trusting of their governments. Since the 1960s, American public trust has declined significantly in the United States government, from three quarters of Americans trusting the government to do the right thing in 1964 to just one quarter by 1997 (Nye, 1997). In surveying the trust of government literature, the United Nations has found that with few exceptions, distrust of government has grown though out the industrialized world (Blind, 2006).

A recent Pew report on public perceptions of government also shows a general lack of trust among Americans for the government, and that the level of trust in the government observed in 2010 was among the lowest observed in the previous fifty years. However, the Pew report also demonstrates that changes in the public's trust of government have not been unidirectional. After bottoming out in the early 90s, American trust in the government rose throughout the mid to late 90s and early 2000s, with a high of approximately 55% trusting the government to do the right thing. Shortly after the September 11th terrorists attacks, trust began a new decline, continuing into the current decade (Pew, 2010).

Across these reports on public trust of the government a range of reasons for lost trust are proposed. Economic conditions may be the most significant factor (Nye, 1997) (Blind, 2006) (Pew, 2010). Not surprisingly, corruption and scandals are also suggested as leading to a loss of trust (Nye, 1997)(Blind, 2006). Additional factors, including partisanship (Pew, 2010) and satisfaction with the results of government action or society in general (Pew, 2010) (Morgeson, VanAmburg, and Mithas, 2010) have also been suggested as factors that impact public trust in government.

Of course, both governments and academics have attempted to discover how trust for the government might be built. One avenue that has been pursued that is relevant to this paper is the use of e-governance; the increased accessibility of government agencies and services via the Internet. Analysis of a 2008 survey found that the use of e-governance services by individuals can positively impact the confidence (a concept closely related to trust) that individuals have for federal agencies (Morgeson, VanAmburg, and Mithas, 2010). A previous survey of Canadian citizens also found that a positive experience associated with the use of an e-governance service can positively impact the trust that an individual has for a government (Parent, Vandebeek, and Gemino, 2005). However, both studies also found that the influence of e-governance services on trust was secondary; e-governance services positively impacted the trust of individuals who already had somewhat high levels of trust (Parent, Vandebeek, and Gemino, 2005)(Morgeson, VanAmburg, and Mithas, 2010).

Aside from measuring trust of the government, the Pew study also examined the related feeling of favorability regarding specific agencies. Here too, there has been a general decline in the levels of positive opinion. However, and not surprisingly, observed feelings of favorability vary significantly based on the specific agency or department being considered. For example, in 2010, 83% of participants expressed favorable feelings towards the Postal Service, while only 40% expressed favorable feelings towards the Department of Education, the least favored department considered. Furthermore, all agencies and departments considered elicited higher levels of favorability than Congress (Pew, 2010). While these findings do not specifically concern trust, they do demonstrate that a related form of public opinion can vary significantly across specific agencies.

The literature discusses a decline in the general trust of government. However, in light of the variability of trust overtime, the differences in opinion among agencies and the government in general, and the generally positive impact that third party input can have on trust (Jøsang, Ismail, and Boyd, 2007), I am hesitant to hypothesize that a government certification will have a negative impact on the trust that users have for a privacy policy summary. Thus, I posit the following hypothesis and research question:

> *H3: Government involvement via oversight will have some significant impact on the trust that individuals have for a privacy information aid.*
>
> *RQ1: Will government involvement via oversight have a positive or negative influence on the trust that individuals have for a privacy information aid?*

Value of Privacy Information Aids

Given the current concern for budgetary matters, the always present issue of funding a potential alternative is especially salient today. Thus, a final set of questions worth consideration and of interest to policy makers relate to financing a potential alternative. All things being equal, a financially self-sustaining alternative would be viewed more favorably by policy makers and implementers. This leads to the question: are individuals willing to pay for privacy information aids?

Several studies show that individuals are willing to pay a price premium of some type in exchange for a greater protection of privacy, especially in situations in which an individual's concern for privacy is high. Analyzing results from several experimental groups, Egelman et al. and Tsai et al. found that survey participants, using their own credit card information, were willing to pay a higher price for goods on websites that indicated higher levels of privacy protection (Egelman, et al., 2009) (Tsai, et al., 2009). Analysis of an experimental study suggested that in a situation in which websites pay individuals for the collection of certain personal data, websites without privacy practices addressing storage errors, improper access, or unauthorized secondary use would need to pay Americans between $30.49 and $44.62 more than websites with privacy practices addressing those issues (Hann, et al., 2007). A 2005 contingent valuation of the New Zealand public's willingness to pay for greater privacy via instituting a personal property right in personal data found that of survey respondents who were willing to pay, the average value they were willing to pay was approximately $28.25 USD (Rose, 2005). Extending the existence of some willingness to pay for privacy protection to privacy information aids, the following hypothesis is proposed:

> *H4: Willingness to pay among the public for privacy information aids will be greater than zero.*

Egelman also found a link between the level of privacy concern and the willingness to pay a price premium, as well as the value of that premium. Across two groups, one purchasing an innocuous item and one purchasing a personal, potentially embarrassing item, significant differences were found in survey participants' level of concern for privacy and willingness to pay, with participants who were asked to purchase the personal item indicating higher levels of concern and a greater willingness to pay for greater privacy protection (Egelman, et al., 2009). The 2005 New Zealand contingent valuation also found a positive correlation between an individual's level of privacy concern and his/her willingness to pay for increased privacy protection via a personal property right in personal data (Rose, 2005). Based on evidence that the level of privacy concern is positively associated with the amount that an individual is willing to pay for privacy protection, the following hypothesis is proposed:

> *H5: Individuals with higher levels of privacy concern will be willing to pay more for privacy information aids.*

It would seem obvious that trust would be positively associated with the amount an individual would be willing to pay for a given good or service. This association is statistically supported in the literature via a study of the impact of reputation systems on consumer trust for sellers and the amount a consumer would be willing to pay for a product from sellers on an online auction site. Based on a field experiment involving buyers and sellers on eBay, researchers found a positive correlation between the price that consumers would pay for an item and the level of trust that consumers perceive in the seller of that item (Ba and Pavlou, 2002). Showing this same association exists regarding privacy protection, the 2005 New Zealand contingent valuation found a correlation between the trust that individuals had for the government and their willingness to pay for government implementation of a personal property right in personal data (Rose, 2005). Extending these findings to privacy information aids, the following hypothesis is proposed regarding willingness to pay and trust:

> *H6: Willingness to pay for a privacy information aid will be positively correlated with the trust that individuals have for the privacy information aid.*

Finally, it is also worthwhile to observe whether the source of a privacy policy summary impacts individuals' willingness to pay, as well as government involvement via auditing. Drawing on the literature mentioned for H6 which links willingness to pay with trust, and the literature cited for H2 and H3, the following hypotheses and research question are proposed as monetary corollaries to H2 and H3:

> *H7: Willingness to pay will be significantly greater for a privacy information aid provided by a third party organization than one created by a first party website.*
>
> *H8: Willingness to pay will differ significantly based on whether the privacy information aid provision is overseen by a government agency.*
>
> *RQ2: Will individuals be willing to pay more or less for a privacy information aid accredited by a government agency?*

Demographics

Several studies demonstrate that demographics, including gender, age, socio-economic status, and previous experiences can impact privacy concerns, trust, and behavioral intentions. By comparing the results from studies in rural & urban Russia with results from similar studies at Harvard and a university in Capetown, South Africa, Gachter et al. found that there is not a significant difference in the level of trust among university students across national & cultural boarders. However, Gachter found that older participants were more likely to trust people than younger participants. Gachter also found that white and blue-collar participants exhibited less trust towards others than university students (Gachter, Herrmann, and Thöni, 2004). Jensen found that previous online experience, including the number of previous purchases made online and previous privacy violations experienced, impacted the privacy behaviors of individuals.

While the impacts of demographic factors on privacy and trust are not the focus of this paper, literature demonstrates that these factors must be accounted for in any study of privacy or trust. Thus, neither a hypothesis nor a research question will be proposed based on demographics. However, demographic factors will be controlled for in the study and analysis conducted for this paper.

Chapter 4 - Methodology

In order to test the hypotheses and research questions posited above, an online survey regarding privacy concerns, trust, and willingness to pay was created and conducted. This chapter will describe the survey methodology employed, the questions used for measuring relevant variables, and the method by which the survey was executed.

Questionnaire

The primary tool of data collection was an online questionnaire created using SurveyMonkey. This questionnaire, described in detail below, included the text of a summary of a website's privacy policy and questions regarding comprehension of that summary, trust in that summary, the willingness to pay of participants for a similar summary, secondary use privacy concerns in general, and demographics. In this questionnaire, the privacy policy summary was used as a proxy for testing questions about privacy information aids more generally. The full questionnaire can be found in Appendix I.

Summary Creation

In order to place survey participants in the mindset of thinking critically about privacy, each participant was presented with a summary of the privacy policy of Match.com. Presentation of a privacy policy summary also allowed for the questionnaire to be framed as a set of questions regarding the summary, making the questionnaire less abstract or hypothetical to participants.

This study made use of a single privacy policy, as opposed to several, for two reasons. First, the primary focus of this study is trust regarding third parties and government oversight, not the content of actual privacy policies. Second, using multiple privacy policies would introduce additional variables, such as the relationship between protectiveness of a privacy policy and the user's level of trust in both the original party and the third party (Vail, Earp, and Anton, 2008) (Schlosser, White, and Lloyd, 2006). This study does not include the proper means for measuring and controlling for these additional variables. Thus, it was thought best to not introduce those variables into the study.

The privacy policy of an actual website was used as the basis for the created summary so that the summary presented to survey participants would be descriptive of a privacy policy that participants were likely to encounter online, and thus be perceived as realistic. The specific website privacy policy used in this study, Match.com, was used as a result of a selection process which included specific criteria for the market sector from which a privacy policy was to be chosen and the specific site from within that sector. In addition, the summary based on Match.com's privacy policy was also created by a process which attempted to emulate a similar process previously undertaken in the literature.

Selecting a Sector

The following criteria (with rationales) were selected for determining which sector a privacy policy would be taken from, based on the needs of research, focus of this study, and concerns for possible over or under influence of associated privacy concerns on the survey:

1. Data about consumer tastes and/or behavior is collected – privacy regarding consumer tastes and behavior are the primary focus of this study;
2. Does not deal primarily with medical data or other data covered by HIPAA – this study does not focus on privacy as it relates to medical data or HIPAA;

3. Engages in a business which does not run afoul of US law – remove the possibility that privacy concerns related to conducting illegal activity would impact survey results;
4. Sector is significant in either American usage or American revenue – so that the policy used in this study can be of relevance to the general American Internet user;
5. Engages in a business in which users are likely to reveal information that they wish to keep private – to increase the likelihood that survey participants will answer questions with the greater care and concern typical of contexts in which privacy is important to a user (Schlosser, White, and Lloyd, 2006) (Beldad, de Jong, and Steehouder, 2010).

Based on these criteria, online dating was selected as the sector from which to select a policy. In filling out their profiles, users are often asked to – and have an incentive to – fill out information regarding their tastes, interests, and habits, addressing criteria 1. At the same time, users of online dating sites are not asked to provide personal health information that is covered by HIPAA, thus meeting criteria 2. As of March 2011, online dating sites are fully legal to operate and use in the United States, thus satisfying criteria 3. In addition, online dating represents a significant US business, with 2010 revenues estimated to be $1.08 billion (Moldvay, 2010) and recent monthly visits to popular sites measuring in the tens of millions, as evident in Table 1, fulfilling criteria 4. Finally, use of online dating sites requires disclosure of information that users may wish to retain a significant level of privacy control over, thus addressing criteria 5. In fact, concerns that friends or family will find out that an individual is listed on an online dating site, as well as concerns about their representation on online dating sites, are found to be significant influences on the privacy protecting behaviors of users of online dating sites (Gibbs, Ellison, and Lai, 2011).

Selecting a Site

In addition to criteria for selecting a sector, criteria were also created for selecting a particular privacy policy to use in this study. The following criteria were used in the selection of a privacy policy from the online dating sector:

1. Company does business in the United States – to be applicable to the focus of this paper, U.S. policy on privacy;
2. Popularity of site – to be representative of sites that users are most likely to encounter;
3. Contains text relevant to secondary use and transfer of user data – to be applicable to the focus of this paper.

Table 2[6] lists three sites that were considered. Noting that Match.com can be considered the most popular of the three sites based on two of the three measures provided, and that the company is located in and does business in the United States, it was decided that this company would be the first to be considered as a source for a privacy policy. Match.com's privacy policy (as of March 13th, 2011) was carefully reviewed and was found to contain a considerable amount of text dedicated to secondary use and transfer of information. In fact Match.com's privacy policy includes lengthy sections dedicated to its practices regarding use and sharing of information (Match.com, "Privacy Statement", 2011).

[6] Sources for the information displayed in Table 2 include (Slutsky, 2011), Alexa (Alexa, "Match.com Site Info", 2011)(Alexa, "Eharmony.com Site Info", 2011)(Alexa, "Zoosk.com Site Info", 2011), and each site's "About Us" page (Match.com, "About Match.com", 2011)(eHarmony.com, 2011)(Zoosk.com, 2011).

Site	Location of Business	Number of Visitors in January 2011 (in millions	Number of Registered Users (in millions)	Alexa Traffic Rank in the United States
Match.com	Dallas, TX	65.4	21.8	81st
eHarmony.com	Pasadena, CA	15	33	330th
Zoosk.com	San Francisco, CA	30.8	60	678th

Table 2 – Location and usage information of three popular dating websites

Creating the Summary

A summary of Match.com's February 8th, 2011 privacy policy was created by the author and can be found in Appendix II. The method employed to create the summary was to read over the full privacy policy and note clauses that fell within a subset of Anton and Earp's privacy goal and privacy vulnerability taxonomies (Anton and Earp, 2004). The subset, shown in Table 3, includes only classifications and sub-classifications dealing with information use or transfer, classifications which fall within the unauthorized secondary use concern. Following the full read though, noted clauses were summarized into two bulleted lists, one summarizing data use practices and the other summarizing data sharing practices. After this, the bulleted lists were rewritten as paragraphs in order to improve readability. In order to remove any influence from reputation or brand loyalty, all references to Match.com and its parent company IAC were replaced with "BrandX" and "ParentCorp", respectively (Vail, Earp, and Anton, 2008).

Protection Goal Taxonomy Subset	**Privacy Vulnerability Taxonomy Subset**
• Notice/Awareness o General Notice/Awareness o Identification of the uses to which the data will be put o Identification of any potential recipients of the data o 3rd party limitations • Choice/Consent o Choice of sharing data	• Information aggregation • Information transfer o Sharing PII with users o Sharing/selling with companies/sites o Limitations of Sharing • Information personalization o Personalization by user preference o Personalization of site and service o Personalization of advertising, offers, and promotions

Table 3 – Subset of Anton and Earp's taxonomies used in summary creation

Comprehension Questions

Three questions were presented to participants alongside the privacy policy summary to gauge whether or not the participant had read the summary. This section was not meant to test the ability of participants to comprehend a policy summary, or to test the effectiveness of the summary as an aid to user comprehension. These questions simply indicate the level of time and effort the participants exercised in completing the reading portion of the questionnaire. Thus, the three questions were designed to be simple to answer for participants who read or referred to the summary. Responses to these questions were not used to screen out respondents. Instead, these questions were used to promote reading of the summary by participants and to identify participants who had not read the summary.

Trust of Summary Questions

Questions were used to gain a subjective/specific measure of survey participants' decision trust regarding the privacy policy summary presented earlier, which is noted as being the most appropriate measure for a survey to target (Jøsang, Ismail, and Boyd, 2007). To observe the subject/specific measure of decision trust, a subset of questions from a study by Mayer and Davis on employee trust of management was adapted and applied to this survey (Mayer and Davis, 1999). Specifically, the study's questions regarding *ability*, *benevolence*, and *integrity* were applied to this survey in order to measure the components that reduce perceived risk in the decision trust framework. These questions were tested and found to be reliable and consistent by Mayer and Davis, with Cronbach alphas[7] of .93, .95, and .96, respectively. Where appropriate, Mayer and Davis's questions were modified to fit the subject of this survey, and in a few instances questions were dropped due to inapplicability to this survey.

Levels for each component of trust were measured by summing responses to the questions measuring that component. A 5 point Likert scale was used to ask participants how much they agreed or disagreed with a given statement (1 = Strongly Disagree, 5 = Strong Agree). Ability and benevolence were both measured by five questions and thus had a maximum value of 25 and a minimum value of 5, while integrity was measured by three questions and thus had a maximum value of 15 and a minimum value of 3. Total trust was measured by summing the values for ability, benevolence, and integrity, and had a maximum value of 65 and a minimum value of 13.

[7] Cronbach's Alpha is a statistical measure between 0 and 1 of the reliability and consistency of a set of questions as they relate to a specific concept or variable. The closer α is to 1, the more likely that a group of questions are testing the same variable, as opposed to testing multiple, separate variables. Generally, $\alpha > .7$ is considered reliable & consistent for surveys (Bland and Altman, 1997).

Contingent Valuation

For contingent valuation measurement, a set of questions was developed based on contingent valuation literature and best practices. Privacy policy summaries may best be viewed as a public good - as they are non-rivalrous – that improves a user's privacy environment. Furthermore, relevant property rights (copyrights on the summaries) are held by non-users. Given these characteristics, questions were developed to test for willingness-to-pay, as opposed to willingness-to-accept (Mitchell and Carson, 1989, pg. 30 – 41).

Regarding the payment vehicle used, contingent valuation questions were presented as a fee added to the website's monthly service fee. An additional fee was chosen because it does not involve the burden of making a payment to a party in addition to current parties, and because it does not carry the political connotations of a tax. Furthermore, the use of a fee from a website as the payment vehicle hypothetically provides greater flexibility to consumers, as they can decide whether or not to accept the service and pay the additional fee.

The payment card method, i.e. providing the participant with a range of values to pick from, was chosen for eliciting values (Mitchell and Carson, 1989). This method was chosen due to its simplicity, the lack of an existing value for privacy policy summaries in the literature on which to base a dichotomous choice question, and a concern that the survey sample would not be large enough to draw a significant conclusion from if dichotomous choice were employed (Mitchell and Carson, 1989). Survey participants were presented with a range of possible responses to the question of how much they would be willing to pay for a privacy policy summary similar to the one that had been previously presented to them. The possible responses ranged from $0.10 to $1.00 in ten cent increments, plus an option of $0.05 and a greater than

$1.00 option. In addition, to capture protest votes, the first contingent valuation question presented to participants asked whether participants were willing to pay any value for the summary (Mitchell and Carson, 1989). Those who indicated an unwillingness to pay were then asked a question to register whether the unwillingness response was a protest vote. Those who indicated a willingness to pay were then presented the payment card willingness to pay question.

Privacy Concern Questions

Four questions, taken from (Smith, Milberg, and Burke, 1996), are used to measure the level of concern that survey participants have for privacy. The full set of fifteen questions developed by Smith et al. resulted from an extensive effort by the authors, which included an exhaustive literature review and multiple stage instrument reliability testing, to create a survey instrument for measuring levels and types of privacy concerns among target populations. In order to limit the length of the survey and stay within the focus of this paper, the questions taken from Smith et al., includes only the set of questions which focus on unauthorized secondary use. Limiting questions to a single aspect of privacy removes the ability to compare participants' ranking of privacy components (i.e., some participants may rank Collection as their greatest concern while others may rank Unauthorized Secondary Use as their greatest concern,) but it does allow for the grouping of participants into subsamples based on their relative concerns for Unauthorized Secondary Use. Smith et al, established the consistency of these questions during their instrument creation process, and reported a Cronbach's alpha of .80 for the Unauthorized Secondary Use questions. Privacy concern questions in this study were be measured via a 5 point Likert scale. As with the measures of trust, the level of privacy concern was measured by summing the responses to privacy concern questions, with 20 being the maximum level of privacy concern and 4 being the minimum.

Demographic Questions

A set of basic demographic questions is included so that the survey sample may be compared to the target population and so that demographic factors may be controlled for in data analysis. Participants were asked for their age, gender, and whether they were an undergraduate or graduate student. Participants were also asked for the highest level of education completed by either of their parents, as a proxy for income.

Experimental Design

To test the hypotheses regarding the effects of first or third party summary creation and the effects of government oversight, a 2 x 2 factorial experiment was conducted (Keppel, 1982). Independent variables in the factorial design were the relationship between the summary author and the website, and whether or not a federal agency, in this case the FTC, performed annual audits of the summary for correctness. To test these independent variables, four subsamples were employed, and each was presented with the previously described questionnaire. Questionnaires were nearly identical across the four subsamples except for text and question wording relevant to the major independent variables. Where appropriate, text and question wording indicated that the summary displayed at the beginning of the questionnaire was written either by “BrandX” or by a third party, academic institution. In addition, where appropriate, text and question wording either made no mention of annual audits by the FTC or indicated that the FTC had performed an annual audit of the summary for accuracy. Appendix III presents the language differences used among the four questionnaires, and PDFs of the four actual questionnaires can be downloaded at http://www.wbushey.com/masters-thesis-materials/.

Survey Execution

Due to time and financial constraints, a convenience sample was used in this survey. Students of the University of Minnesota Twin Cities (UMNTC) campus were designated as the target population for this study. In addition to its convenience (a representative sample could be obtained by emailing a random subset of University students), this population was chosen because of the high representation of members of this age group (generally late teens to early thirties) in online environments.

A preliminary, informal survey was conducted on April 14th, 2011 in order to establish the range of values to present to survey participants in the contingent valuation question. This survey was distributed by posting a URL to a SurveyMonkey survey which contained only the willingness to pay questions on the author's social network accounts (Facebook and Twitter). 51 completed preliminary surveys were collected. Based on these collected responses, the range of values in the contingent valuation question was adjusted to its current range.

Formal data collection occurred by creating four SurveyMonkey surveys, each representing one of the four experimental treatments of the 2 x 2 factorial design. Recruitment occurred by random, cold emailing of sample frames of UMNTC students. A list of email addresses for all UMNTC students who had not elected to keep their email address private was obtained via a public records request though the University of Minnesota's Office of Institutional Research. From this list of over thirty three thousand email addresses, sample frames of 375 emails were randomly selected for each treatment. Addresses in the sample frames were sent a cover email (Appendix IV) introducing the survey, explaining its purpose, informing individuals that they were not compelled to take the survey, and providing a link to the survey. To increase response rates, two reminder emails were sent to addresses which had not completed surveys. In addition, individuals who completed the survey were entered into a random drawing, conducted on May 31st, 2011, for a $25 gift certificate to Amazon.com. Individuals were informed of this random drawing, and the fact that information about how they could protect their privacy online would be presented to them following completion of the survey, in the cover email as a means to increase response rates. A Java program was written and used to handle the random selection of email addresses for samples, the sending of emails, and the selection of a winner for the random drawing[8].

Upon clicking the URL provided in the email, individuals were taken to the survey, where they were presented with an informed consent form. This form described what the respondent would be asked to do during the survey, informed the respondent that no personal information would be collected about him/her, and again informed the respondent that he/she was not compelled to start or finish the survey. Terms for the gift certificate random drawing were also again described. Following this disclosure, respondents were asked if they consented to participation in the survey. Those replying affirmatively were taken to the first page of the survey instrument, while those replying negatively were presented with an exit page. During the survey, the orderings of questions within the trust and privacy concern sections were randomized so as to minimize the effects of ordering bias (Alreck and Settle, 2004).

[8] The source for this program is available for download at http://www.wbushey.com/masters-thesis-materials/ .

The formal survey was conducted from April 25th, 2011 to May 9th, 2011. Emails were sent to the first four sample frames, totaling 1,500 email addresses, on April 25th. Reminder emails were sent to those who had not yet completed the surveys on April 27th and April 29th. This process was repeated on May 2nd with a new group of 1,500 randomly selected student email addresses (with the previous 1,500 removed from random selection). Reminder emails were sent to the second group on May 4th and May 6th. Partially completed responses were removed before each batch of emails was sent. Response collection was closed on May 9th by deactivating the survey URLs. In total, 3,000 random individuals were randomly emailed, with 261 completed surveys collected for a final response rate of 8.7%.

Chapter 5 - Analysis & Results

Having collected data as described in the previous chapter, this chapter will present data analysis and its results for the questions posed earlier about the relationships between privacy concern, trust, first party status, government oversight, and willingness to pay among the public as they relate to the provision of privacy information aids. First, preparation that occurred to the data will be described, followed by a basic breakdown of the demographics of the collected data. Following this will be an in-depth analysis of the data, which relies heavily on mathematical techniques of analysis of variance and regression analysis. Next, the results from this analysis for the previously stated hypotheses and research questions will be discussed. Finally, the limitations of the present study will be presented.

Data Preparation

Before analysis could occur, the data collected from the SurveyMonkey questionnaires had to be cleaned and prepared in Excel and then imported into Stata. Columns containing unneeded, and often empty, values were deleted. Each column was given a variable name. Summations were created for the following groups of questions using Excel's SUM function: Ability trust, Benevolence trust, Integrity trust, Total Trust, and Privacy Concern. In addition, variables were created to indicate if a respondent correctly responded to each of the comprehension questions. A listing of all the variables created and used during analysis can be found in Appendix V. In the case of the dichotomous variables CV_WTP, CV_Protest, DEMO_Gender, and DEMO_Degree, 1 was subtracted from the recorded responses so that the data would conform to the conventional values of binary variables, 0 and 1, instead of the values recorded by SurveyMonkey, 1 and 2. For the willingness to pay valuation question, the choice numbers recorded by SurveyMonkey were converted into the monetary values represented by a given choice.

Each subsample had one respondent who did not consent to take the survey, and as a result did not respond to the questionnaire. These non-consent entries were deleted. Following this deletion, the smallest subsample had 59 respondents. To allow for cross sample analysis, the other samples were reduced in size so that all samples had the same number of respondents. This was done by randomly sorting entries in Excel and deleting the appropriate number so that each subsample had 59 respondents. Following this, each sample was imported into Stata by copying and pasting the data into Stata's Data Editor.

Demographics

	Age Mean	**Age Std. Dev.**	**Gender**	**Degree Sought**	**Parents' Ed Level Mean**	Parents' **Ed Level Std. Dev.**
First Party Not Reviewed	24.12	6.07	Male: 44.07% Female: 55.93%	Undergrad: 77.88% Graduate: 22.12%	4.90	1.46
First Party Reviewed	23.14	4.52	Male: 30.51% Female: 69.49%	Undergrad: 62.72% Graduate: 37.28%	5.15	1.40
Third Party Not Reviewed	24.40	6.14	Male: 38.98% Female: 61.02%	Undergrad: 64.41% Graduate: 35.59%	5.27	1.34
Third Party Reviewed	23.79	5.92	Male: 47.46% Female: 52.54%	Undergrad: 64.41% Graduate: 35.59%	4.98	1.43
All	23.86	5.68	Male: 40.24% Female: 59.76%	Undergrad: 66.10% Graduate: 33.90%	5.08	1.41

Table 4 - Sample Demographics

Table 4 presents the demographic information for each treatment subsample and the total study population. In comparing the samples to each other, age and parents' education levels appear to be consistent across all the samples. Gender distributions appear to vary significantly, with nearly 70% of the first party/reviewed sample being female while only a little over half of the third party/reviewed sample participants are female. The distribution of undergraduate vs. graduate students is fairly consistent across samples, with the exception of the first party/not reviewed sample, which contains a significantly greater representation of undergraduate students.

Some of these statistics can be compared to official measures published by the University of Minnesota's Office of Institutional Research (OIR) (Office of Institutional Research, 2011). While the OIR does not publish average ages or a continuous distribution of ages, it does provide student counts for various age groups. These counts (under 21: 15,857; 21 – 24: 15,755; over 24: 18,432) suggest that the average age of UMNTC students is likely to be around 24, and that the collected samples are representative of the campus by this measure. OIR's published distribution of gender (female: 51.6%; male: 47.4%; unknown: 1.0%) indicates that the collected samples, with the exception of the third party/reviewed sample, are significantly over representative of the female population of the campus. OIR's published statistics for degree registration show that 63% of degree perusing students are undergraduates and 37% are graduate or professional students, indicating that the first party/not reviewed sample is significantly over representative of undergraduate students, while the other samples are fairly representative. OIR does not publish statistics on the education levels of students' parents; thus those statistics cannot be compared.

Data Analysis

The hypotheses stated earlier were subjected to statistical hypothesis testing, which is based on a combination of proof by contradiction and probability. For each hypothesis, a null hypothesis representing the negated claim is created and assumed. Because all of the hypotheses stated in this paper claim that some variable will have a significant impact on either trust or valuation, all of the null hypotheses assume that the variable in question has zero impact. Under this assumption, a value is derived based on the collected data for the impact of the variable in question, as well as some measure of the general error or variance observed in the data or an equation. A ratio of the variable's impact and the general error/variance, based on collected data, is used to create some form of score: F, t, χ^2, or Z. Each type of score varies in its ratio definition and which probability distribution it works with, but all represent the same concept: a comparison of the impact of the variable observed in the collected data to the general error or variance observed in the collected data. The created score is then compared to a probability distribution and the following question is asked: what is the probability of observing the created score in a random sample, assuming the null hypothesis is true. If the probability is sufficiently low, the null hypothesis is rejected.

In general, probabilities of 0.10, 0.05, or 0.01 are considered sufficiently low to reject a null hypothesis. However, these cut off values also include different probabilities of either falsely rejecting a null hypothesis or falsely not-rejecting a null hypothesis testing[9]. Thus, it is common for studies to not strictly define the cut-off value employed. Instead, studies often observe when these probability cut-offs are reached, and indicate these observations as

[9] In a proof by contradiction, a null hypothesis can never be accepted, as the proof cannot provide the logical or mathematical evidence required to accept the null hypothesis.

evidence that the null hypothesis must be false with some level of confidence based on the probability cut-off reached (0.10 = 90% confidence level, 0.05 = 95%, and 0.01 = 99%). In instances in which the null hypothesis is that the variable has no significant impact on some measure, reaching some probability cut-off is generally interpreted as the variable being significant at the appropriate confidence level. Following this method, observations and evidence are considered as a whole so that the study may draw conclusions regarding what is highly likely to be true. This is the method of analysis employed in this study.

For convenience and reference, the hypotheses and research questions stated above are listed below. In addition, Table 5 describes the conventions that will be used for indicating statistical significance in the results that follow.

> *H1: An individual with a high level of concern for privacy will have a low level of trust for parties that provide privacy information aids.*
>
> *H2: Users are statistically more likely to trust a privacy information aid created by a third party organization than one created by a first party.*
>
> *H3: Government involvement via oversight will have some significant impact on the trust that individuals have for a privacy information aid.*
>
> *H4: Willingness to pay among the public for privacy information aids will be greater than zero.*
>
> *H5: Individuals with higher levels of privacy concern will be willing to pay more for privacy information aids.*
>
> *H6: Willingness to pay for a privacy information aid will be positively correlated with the trust that individuals have for the privacy information aid.*
>
> *H7: Willingness to pay will be significantly greater for a privacy information aid provided by a third party organization than one created by a first party website.*
>
> *H8: Willingness to pay will differ significantly based on whether the privacy information aid provision is overseen by a government agency.*
>
> *RQ1: Will government involvement via oversight have a positive or negative influence on the trust that individuals have for a privacy information aid?*

RQ2: Will individuals be willing to pay more or less for a privacy information aid accredited by a government agency?

Superscript	Meaning
*	Significance in the hypothesized direction at the 90% confidence level.
**	Significance in the hypothesized direction at the 95% confidence level.
***	Significance in the hypothesized direction at the 99% confidence level.
=	Significance in the unhypothesized direction at the 90% confidence level.
==	Significance in the unhypothesized direction at the 95% confidence level.
===	Significance in the unhypothesized direction at the 99% confidence level.
Note:	In the following analysis, significance of t-scores for CONCERN_Sum and firstParty are based on one-tailed tests. Significance of t-scores and Z-scores for all other variables is based on two-tailed tests.

Table 5 - Convention Used to Indicate Significance via superscripts

Trust Hypotheses

ANOVA (ANalysis Of VAriance) and regression analyses were performed in Stata 11.1 in order to test these hypotheses. Before testing hypothesis H1, an analysis was performed for hypotheses H2 and H3 via ANOVA modeling, which allows for testing of significant differences among data points that have been grouped by some variable. ANOVA modeling is particularly useful in a factorial experiment in which the independent variables take on discrete values, and is thus employed for hypotheses H2 and H3.

ANOVA

	One-way: firstParty	One-way: reviewed	Two-way
Adjusted R^2	0.0253	-0.0042	0.0194
Model	7.09^{***}	0.03	2.55^{*}
firstParty	7.09^{***}	---	7.05^{***}
Reviewed	---	0.03	0.03
firstParty & reviewed	---	---	0.57

Table 6- Statistics from ANOVAs on TRUST_Sum

Table 6 displays the F-scores resulting from three ANOVA commands performed for TRUST_Sum on each independent variable of interest. One-way ANOVA allows for the testing of significant differences among groups identified by only one variable, while two-way ANOVA allows for testing of significant differences among groups identified by two variables. In the case of two-way ANOVA, the potential for significant differences caused by interactions among the two variables – in which the impact of one of the independent variables may be dependent on the value of the other independent variable – must also be tested for, resulting in the need for the right most column (Keppel, 1982). These three ANOVA results show a significant difference among groups based on whether the summary author was a first or a third party, but not significant difference between groups based on whether or not the summary was reviewed by a federal agency nor a significant difference resulting from an interaction between the two variables.

	TRUST_ABILITY_Sum	TRUST_BENEVOLENCE_Sum	TRUST_INTEGRITY_SUM
Adjusted R^2	0.0107	0.0181	0.0053
Model	1.84	2.44^{*}	1.42
firstParty	5.10^{**}	6.84^{***}	3.22^{*}
Reviewed	0.14	0.10	0.31
firstParty & reviewed	0.29	0.39	0.73

Table 7 - F-scores from ANOVAs on each component of trust

As trust was actually measured as a sum of three components, ANOVA analysis was also performed with the components serving as dependent variables instead of total trust. This analysis allows one to examine differences in impact among the three components: *ability*, *benevolence*, and *integrity*. Table 7 displays the results of the two-way ANOVA executions on each of the three components. One-way ANOVAs were not run on the components as doing so appears to be of little use given the extreme differences in significance between the two variables. As with total trust, significant differences only appear to exist among groups divided by the first/third party status of the summary's author. Notably, the level of this significance varies with the component of trust, suggesting that the first/third party status of a summary author may have the greatest impact on benevolence, and the least impact on integrity.

Regression Analysis

Regression analysis was used to test the hypothesis regarding privacy concern and trust, and to further investigate hypotheses H2 and H3, which focus on the role that first or third party status has on trust of privacy information aids and the role government oversight has on trust of privacy information aids. Like ANOVA analysis, regression analysis can be used to observe significance. However, while ANOVA observes significant differences between groups, regression analysis observes significant influence of statistical models and the independent variables in those models. Thus, regression analysis allows for a finer and more complex level of analysis of data.

EQ1: $$\text{TRUST\_Sum} = \beta_0 + \beta_1\text{CONCERN\_Sum} + \beta_2\text{firstParty} + \beta_3\text{reviewed} + \beta_4\text{DEMO\_Age} + \beta_5\text{DEMO\_Gender} + \beta_6\text{DEMO\_Degree} + \beta_7\text{DEMO\_ParentEd} + \varepsilon$$

To test hypotheses H1, H2, and H3, EQ1 was constructed and regressed upon, which explains the level of trust a respondent reported as a linear function of the respondent's level of concern for privacy, whether the privacy information aid was provided by a first or a third party, whether the privacy information aid was reviewed by the FTC, and the demographic variables measured by the questionnaire. It should be noted that in EQ1, the coefficients on the firstParty and reviewed binary variables represent differences in the average levels of measured trust between the first/third party and reviewed/unreviewed treatments (Studenmund, 2006).

Differences in slopes resulting from the different treatment conditions are not included in EQ1, as there is no reason to believe that an interaction exists between either the first/third party variable and the other variables or the reviewed/unreviewed variable and other variables. A regression was run on a modified version of EQ1, which included slope binary variables, to test for these interactions. Results for this regression, shown in Figure H of Appendix VI, support the belief that significant interactions do not exist.

Statistics from the regression of EQ1 are shown in Table 8, which demonstrate that the equation, while jointly significant, leaves plenty of room for improvement. An attempt to improve the quality of this first equation was made by removing irrelevant variables and modifying the structural form of the variables. Based on the statistics from the regression of EQ1, and reflection on what the variables represented, DEMO_Degree and DEMO_ParentEd were dropped from the equation. DEMO_Degree was considered to be irrelevant and was verified to be redundant given the presences of the DEMO_Age variable. In the case of DEMO_ParentEd, the variable's lack of significance may indicate that the level of education of an individual's parents may not be the proper measure of socio-economic status for a student regarding Internet issues. Significance of the DEMO_ParentEd variable may also be hampered by the distribution of respondents; upon examination of the variable, it was found that nearly two-thirds of respondents were children of a parent with at least a bachelor's degree. Finally, the structure of the relationship between CONCERN_Sum and TRUST_Sum was further analyzed by substituting CONCERN_Sum with its natural log. The use of a logarithm in a regression represents the impact that a 1% change in the independent variable has on the dependent variable. This differs from the linear structure usually used in regression, which represents the impact of a one unit change. Substitution of CONCERN_Sum by its natural log, CONCERN_Sum_ln, did have a noticeable impact on the significance of that variable.

The refined trust equation used for regression analysis, EQ2, is listed below. Results from a regression of this equation are shown in Table 8.

EQ2: $$\text{TRUST\_Sum} = \beta_0 + \beta_1\ln(\text{CONCERN\_Sum}) + \beta_2\text{firstParty} + \beta_3\text{reviewed} + \beta_4\text{DEMO\_Age} + \beta_5\text{DEMO\_Gender} + \varepsilon$$

		EQ1	**EQ2**
Adjusted R^2		0.0458	0.0542
Model F-score		2.60^{**}	3.67^{***}
t-scores	CONCERN_Sum	0.85	$1.32^{=}$
	firstParty	-2.63^{***}	-2.61^{***}
	Reviewed	-0.07	-0.17
	DEMO_Age	-1.67^{*}	-2.92^{***}
	DEMO_Gender	-1.44	-1.42
	DEMO_Degree	-0.68	---
	DEMO_ParentEd	-0.26	---

Table 8 - Statistics from Regressions on EQ1 and EQ2

The results of the above regression suggest a few conclusions. The hypothesis that privacy concern negatively impacts trust of a privacy information aid is not supported, as the data does not show a significant negative impact from privacy concern. In fact, privacy concern may have the opposite impact, as it appears to be significant in the positive direction in the refined trust equation. The hypothesis regarding the positive impact third party status has on trust seems to be further supported by regression analysis, with third party authors being significantly more trusted than first party authors at the 99% level. However, the hypothesis that government oversight would have an impact on trust is fully unsupported by the data;

government review seems to register virtually no impact on the level of trust respondents had for the privacy policy summaries.

As with the ANOVA analysis above, regression analysis of potential interactions and impacts on each component of trust were also performed. Table 9 displays the t-scores and F-scores resulting from regressions performed to test for interactions among the independent variables on TRUST_Sum. Columns represent the specific sample regressed upon. For example the "All" column displays the results of the regression performed with neither of the factorial variables held constant (thus including the entire study sample,) while the "Reviewed" column displays the results of the regression with the reviewed variable fixed to 1 and the firstParty variable keep free (thus including only those respondents who saw a reviewed summary.) Table 10 displays the t-scores and F-scores resulting from regressions of total trust and the three components of trust: *ability, benevolence, and integrity*. Table 11 displays the t-scores and F-scores for regressions performed to test for interactions across the three components of trust.

	All	Reviewed	Not Reviewed	First Party	Third Party
F-score	3.67^{***}	5.88^{***}	0.75	1.53	1.99
CONCERN_SUM_LN	$1.32^{=}$	0.79	1.12	1.19	0.78
firstParty	-2.61^{***}	-1.31^{*}	-2.47^{***}	---	---
Reviewed	-0.17	---	---	-0.73	0.22
DEMO_Age	-2.92^{***}	-0.65	-3.89^{***}	-2.14^{**}	-2.10^{**}
DEMO_Gender	-1.42	-0.64	-1.17	0.13	-1.94^{*}

Table 9 – Statistics from Regressions Across Samples

	Total Trust	Ability Trust	Benevolence Trust	Integrity Trust
F-score	3.67^{***}	3.06^{**}	4.28^{***}	1.72
CONCERN_SUM_LN	$1.32^{=}$	$2.46^{===}$	0.51	0.25
firstParty	-2.61^{***}	-2.15^{**}	-2.64^{***}	-1.76^{**}
Reviewed	-0.17	0.12	-0.66	0.32
DEMO_Age	-2.92^{***}	-1.35	-3.69^{***}	-2.29^{**}
DEMO_Gender	-1.42	-1.73^{*}	-1.17	-0.58

Table 10 – Statistics from Regressions Across Each Component of Trust

Ability Trust	All	Reviewed	Not Reviewed	First Party	Third Party
F-score	3.06**	3.40**	1.41	1.08	1.64
CONCERN_SUM_LN	2.46$^{===}$	1.61$^{=}$	1.86$^{==}$	1.59$^{=}$	1.94$^{==}$
firstParty	-2.15**	-1.76**	-1.23	---	---
Reviewed	0.12	---	---	-0.25	0.30
DEMO_Age	-1.35	-2.34**	0.31	-1.16	-0.82
DEMO_Gender	-1.73*	-1.48	-0.80	-0.71	-1.62

Benevolence Trust	All	Reviewed	Not Reviewed	First Party	Third Party
F-score	4.28***	5.54***	1.12	1.94	3.05**
CONCERN_SUM_LN	0.51	0.47	0.28	0.88	-0.08
firstParty	-2.64***	-2.42***	-1.38*	---	---
Reviewed	-0.66	---	---	-1.05	-0.24
DEMO_Age	-3.69***	-3.94***	-1.59	-2.47**	-2.91***
DEMO_Gender	-1.17	-0.97	-0.53	068	-2.23**

Integrity Trust	All	Reviewed	Not Reviewed	First Party	Third Party
F-score	1.72	4.62***	0.13	0.72	1.08
CONCERN_SUM_LN	0.25	0.67	-0.20	0.42	-0.02
firstParty	-1.76**	-2.10**	-0.64	---	---
Reviewed	0.32	---	---	-0.41	0.75
DEMO_Age	-2.29**	-3.80***	-0.04	-1.62	-1.69*
DEMO_Gender	-0.58	-0.22	-0.28	0.27	-0.98*

Table 11 - Interaction Regressions for each Component of Trust

Analyses for interaction and impact on the components of trust reveal a few interesting observations. In Table 9, it is noteworthy that the refined trust equation is jointly significant only on the subsample of respondents who were presented with a summary that had been reviewed by a government agency or on the entire study sample. Table 10 and Table 11 demonstrate that the refined trust equation fails to be jointly significant in nearly every case of integrity trust, except when regressed on the subsample of individuals who were told that they read a reviewed summary. Furthermore, the impact of privacy concern on trust appears to only be significant in a few instances, where it is significant in the direction opposite that which was hypothesized.

Beyond these observations, analysis of the interaction of factorial variables and the components of trust largely reinforces the conclusions from previous analyses. With a few exceptions, the first party status of a privacy information aid provider continues to significantly reduce the trust that respondents have for the privacy information aid provider. Furthermore, whether or not the privacy information aid is reviewed by the FTC is insignificant in every case. Finally, privacy concern continues to not have a significant negative impact on trust, and appears to actually have a positive impact in certain cases.

Willingness to Pay Hypotheses

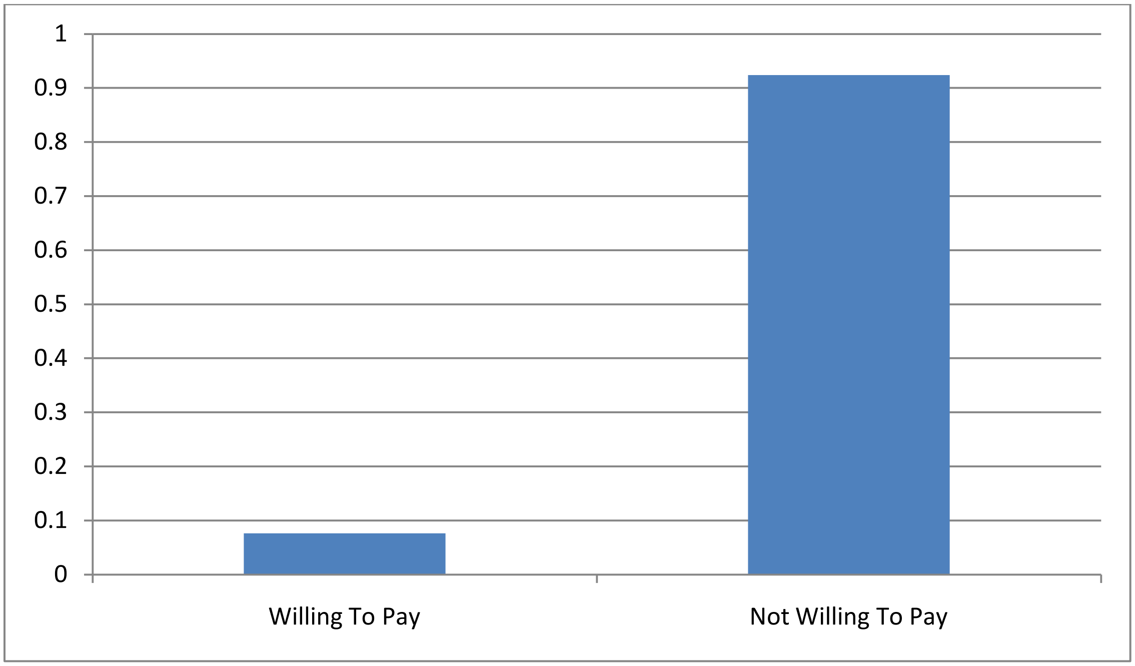


Figure 3 - Percentage of Respondents Willing To Pay for Summaries

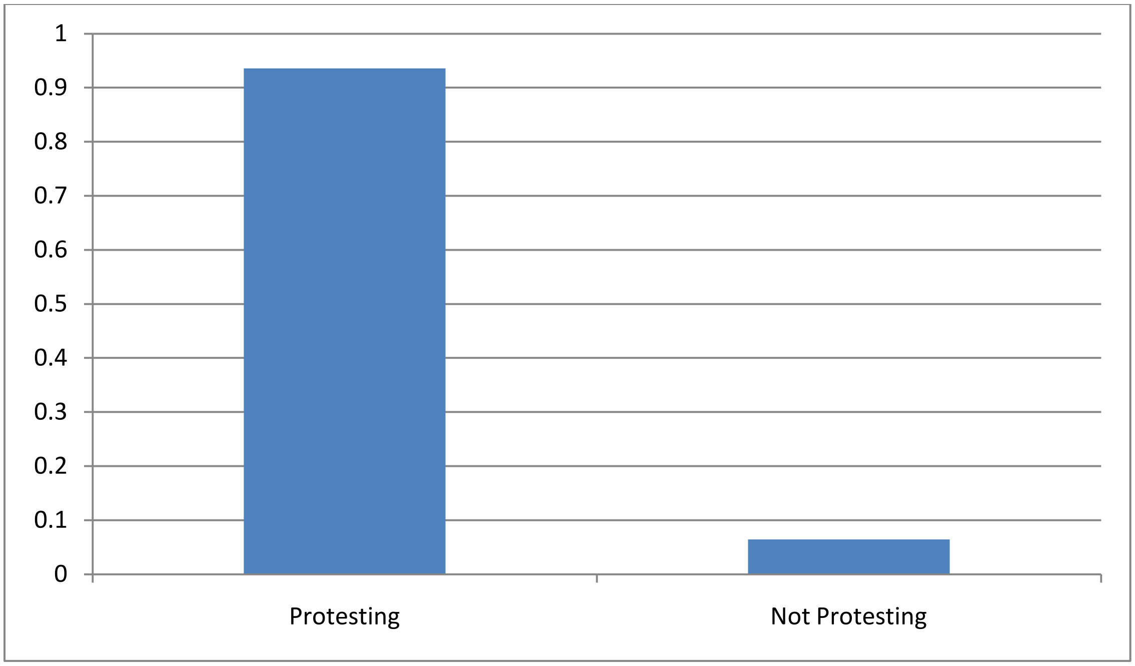


Figure 4 - Percentages of Non Willing to Pay Respondents Who Protest

Figure 3 displays the percentages of responses to the question of whether respondents would be willing to pay any amount for a privacy policy summary. Figure 4 displays the percentages of responses to the question of, among those respondents who indicated they would not be willing to pay, whether respondents felt that individuals should have to pay for a privacy policy summary. For the willingness to pay any value question, 7.62% were willing to pay some amount and 92.38% were unwilling to pay. Of those 92.38% who were unwilling to pay, 93.58% indicated that they felt they should not have to pay for summaries of privacy policies. Together, this indicates that 86.45% of all respondents felt that individuals should not have to pay for a privacy information aid. Interpreted another way, 86.45% of respondents felt that these privacy information aids should be provided for free to users.

The fact that only 7.62% of respondents were willing to pay any price, and that 86.45% felt that the summaries should be provided for free, does not support the hypothesis that the public will be willing to pay a greater than zero amount for privacy information aids. In fact, these results suggest the opposite – that the vast majority of respondents are completely unwilling to pay for a privacy information aid or feel that privacy information aids should be provided for free. Yet in the aggregate, there is some non-zero willingness to pay. Table 12 shows the average valuation across both the subsample that was willing to pay and the entire sample. Furthermore, a t-test was run to test the hypothesis that average valuation would be greater than zero across the entire sample, the results of which (t = 3.3240^{***}) showed that the average valuation across the entire sample was significantly greater than 0. This result supports the hypothesis the public is willing to pay some amount for the provision of privacy information aids.

	Average Valuation (in USD)
Willing to Pay Respondents	0.43
All Respondents	0.03

Table 12 - Average Valuation among respondents who were willing to pay, and among all respondents

Adding further uncertainty to this analysis, the $0.43 average valuation among those who indicated they would be willing to pay is based on a small sample of just 18 respondents spread across four treatment subsamples. This small sample limits the conclusions that can be drawn via statistical testing. Highlighting this is the wide, 95% confidence interval reported for the mean valuation among those willing to pay of $0.25 to $0.61, meaning that the true valuation among those college students who are willing to pay likely lies between those two values.

Furthermore, as a result of the small number of respondents who indicated a willingness to pay, the ability to analyze the data regarding the remaining hypothesis is quite limited. The data provides two candidates for dependent variables in an analysis regarding the remaining hypotheses: the valuation of each respondent and the willingness to pay of each respondent. However, both present significant problems due to the distribution of the collected data. In the case of valuation, as already noted, the small sample size on which an analysis can occur means it will be difficult to draw statistically sound conclusions regarding the impact of each variable. In the case of willingness to pay, the disparity in yes vs. no responses means that analysis of a binary dependent variable will be dominated by the majority responses (no) and will also face difficulty in drawing significant conclusions regarding which variables impact the likelihood that a respondent would be willing to pay or not (Studenmund, 2006).

These difficulties are highlighted in the results below of statistical tests run regarding hypotheses H5, H6, H7, and H8, which focus on the impact that privacy concern, trust, first party status, and government oversight have on the public's willingness to pay for privacy information aids. As with the trust hypotheses, ANOVA was performed as a component of analysis for hypotheses H7 and H8. ANOVA was performed for both of the candidate dependent variables, and in the case of valuation, ANOVA was run on both the subsample of all respondents and the sample of only respondents who were willing to pay. Statistics from these ANOVA are presented in Table 13.

	CV_Value_f, all respondents	CV_Value_f, willing to pay respondents	CV_WTP
Adjusted R^2	-0.0013	0.602	-0.0078
Model	0.90	1.36	0.40
firstParty	2.19	1.16	0.95
reviewed	0.50	2.72	0.24
firstParty & reviewed	0.0	0.08	0.00

Table 13 - Statistics from ANOVA run for H7 and H8

Regressions were also run as part of the analysis of hypotheses regarding the impact that privacy concern, trust, first party status, and government oversight have on the public's willingness to pay for privacy information aids. The hypothesis that trust impacts willingness to pay was analyzed via EQ3 and EQ4, which explain valuation and likelihood to be willing to pay as a simple correlation with trust. Hypotheses regarding the impact of privacy concern, first party status, and government oversight were analyzed via EQ 5 and EQ6, which are valuation and willing to pay corollaries of EQ2, the refined trust equation. For EQ4 and EQ6, as the dependent variable is binary, logistic regression (logit) via maximum likelihood was performed instead of traditional linear regression via ordinary least squares, as logit modeling corrects for the structural defects inherent in the use of linear regression on a binary dependent variable (Studenmund, 2006). Statistics from regressions on these equations are presented in Table 14 and Table 15.

EQ3: $\text{CV\_Value\_f} = \beta_0 + \beta_1\text{TRUST\_Sum} + \varepsilon$

EQ4: $\text{CV\_WTP} = \beta_0 + \beta_1\text{TRUST\_Sum} + \varepsilon$

EQ5: $\text{CV\_Value\_f} = \beta_0 + \beta_1\ln(\text{CONCERN\_Sum}) + \beta_2\text{firstParty} + \beta_3\text{reviewed} + \beta_4\text{DEMO\_Age} + \beta_5\text{DEMO\_Gender} + \varepsilon$

EQ6: CV_WTP = $\beta_0 + \beta_1$ln(CONCERN_Sum) + $\beta_2$firstParty + $\beta_3$reviewed + β-$_4$DEMO_Age + β_5DEMO_Gender + ε

	EQ 3 All Respondents	EQ 3 Willing to Pay Respondents	EQ 4 All Respondents (Z-score)
Adjusted R^2 or Psuedo-R^2	-0.0030	-0.0136	0.0267
F-score or χ^2	0.31	0.77	3.40^*
TRUST_Sum	0.55	-0.88	1.82^*

Table 14 - Statistics from regressions on EQ3 and EQ4

	EQ 5 All Respondents	EQ 5 Willing to Pay Respondents	EQ 6 All Respondents (Z-score)
Adjusted R^2 or Psuedo-R^2	0.0084	-0.0867	0.0478
F-score or χ^2	1.40	0.73	6.06
ln(CONCERN_Sum)	-1.61^*	-0.10	-1.36^*
firstParty	-1.45^*	-1.03	-0.92
reviewed	0.88	1.42	-0.31
DEMO_Age	1.14	-0.35	1.75^*
DEMO_Gender	-0.44	0.06	-0.59

Table 15 - Statistics from regressions on EQ5 and EQ6

As was predicted by the earlier discussion, analysis of the hypotheses regarding the impact that privacy concern, trust, first party status, and government oversight have on the public's willingness to pay for privacy information aids is inconclusive. With few exceptions, ANOVA and regressions produced insignificant results. Furthermore, in every case, the equation or model being analyzed was found to be jointly insignificant, and the R^2 or pseudo-R^2 values were very low. Thus, regressions of the equations and models on the available data do not provide significant evidence regarding any of the hypotheses in question, which is not surprising given the distribution of the data involved. Of the few significant results observed, inconsistency across regressions and the poor joint significance/fit of the regressions means that conclusions cannot be drawn from those variables that appear to be significant.

Results

Results of Hypotheses

Regarding H1, the stated hypothesis that a high level of privacy concern will negatively impact the trust of an individual for a privacy information aid, is not supported by the data; higher levels of privacy concern do not appear to negatively impact the trust of privacy information aid providers. In fact, the analysis suggests that if privacy concern is significant in anyway, it is in a way opposite that which was hypothesized. Such a suggestion is surprising, and indicates at least two possibilities. One is that a problem may exist with the survey instrument, the collected data/sample, or the data analysis performed. The other possibility is that this finding is reflecting an actual phenomenon – individuals with high privacy concern place higher levels of trust in parties that attempt to aid their privacy than individuals with low privacy concern – that was not observed in the literature reviewed for this study.

The results for H2 and H3 are considerably simpler to interpret. The hypothesis that a third party provider of a privacy information aid will be more trusted than a first party provider appears to be supported by the data; a third party author of a privacy policy summary is trusted at a significantly higher level than a first party author. The hypothesis that government oversight will impact the trust individuals have for privacy information aid providers is unsupported; the involvement of a federal agency via auditing summaries of privacy policies does not appear to have any impact on trust.

The result of the question of whether the public is willing to pay for privacy information aids or not depends on what is of most interest to the reader. If the interest is in understanding the public support of directly financing the provision of privacy information aids, then the data appears to show that there is very little support. If the interest is in understanding the aggregate valuation as a suggestion of the revenue that may be available to fund such a service, even if only funded by the minority who are willing to pay, then the data is inconclusive beyond establishing the nearly self-evident fact that the aggregate willingness to pay is greater than zero.

Finally, the remaining hypotheses regarding the impact of privacy concern, trust, first party status, and government oversight on the valuation or willingness to pay of individuals have inconclusive results. These results are inconclusive due to the small number of respondents who indicated that they were willing to pay and provided a valuation. Thus, the collected data cannot be used to understand the relationships of interest to these remaining hypotheses.

Results of Research Question

Both research questions assume supportive findings for hypotheses regarding the significant impact of government involvement on trust and willingness to pay/valuation (H3 and H8). As neither of these hypotheses were supported, investigation of RQ1 and RQ2, concerning the positive or negative impact that government oversight has on trust and willingness to pay of individuals for privacy information aids, is moot. There is no reason to analyze the direction of a variable's influence if there is no evidence to support that the variable in question has any significant influence. Thus, the results regarding the research questions are that these questions can not currently be investigated or tested.

Limitations

Given the largely inconclusive results of data analysis, it is important to consider what factors might have contributed to the observed results and to discuss the limitations that exist in the present study.

Privacy Concern

The negative result for the first hypothesis, concerning the impact that levels of privacy concern will have on trust of the information aids, is especially troubling given that analysis of the collected data suggests levels of concern may actually have a significant impact in the direction opposite that hypothesized based on literature. Such a strongly negative result suggests the existence of one or several severe problems with the conducted study.

When searching for sources of trouble in data analysis, the first step is typically to look at the data itself. In the case of measured privacy concern, the distribution of measured concern, displayed in Figure 5, suggests a problem: there is not enough variability in the collected data to allow for a meaningful regression analysis.

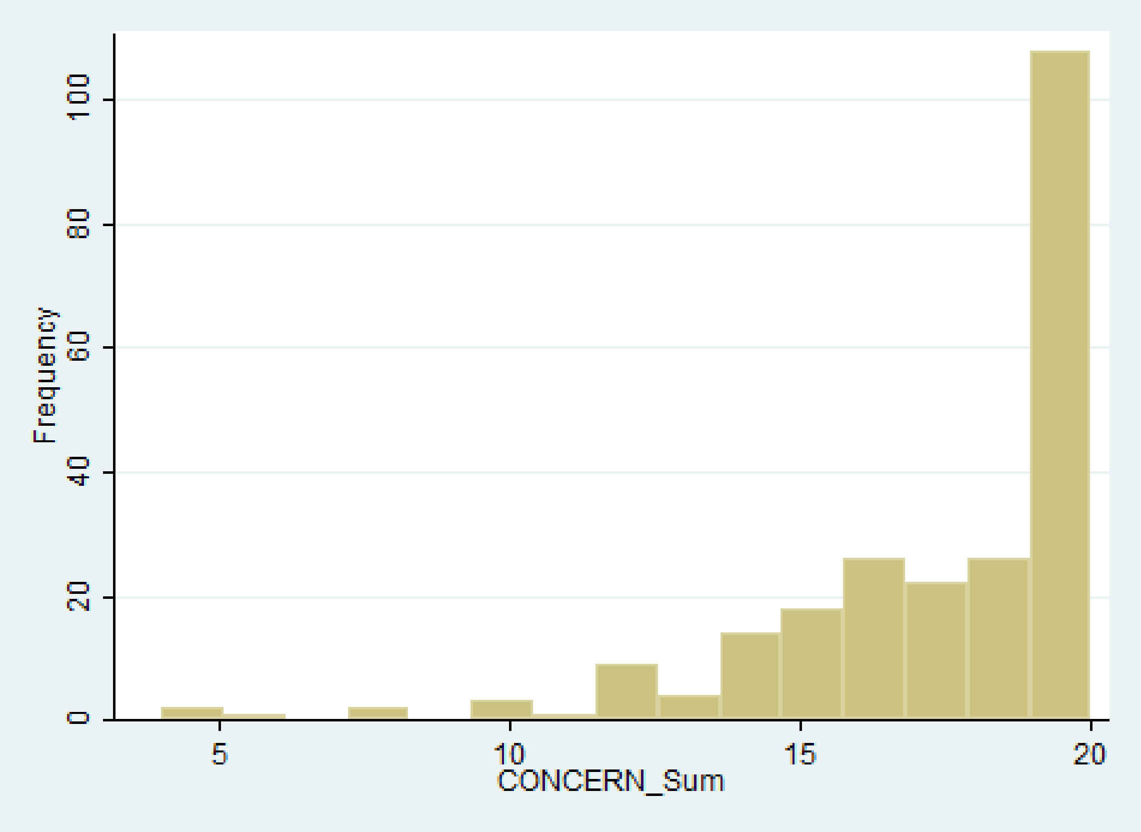


Figure 5 - Distribution of measured privacy levels

Across his many studies of privacy concern, Westin found that levels of concern usually followed a normal distribution, with privacy fundamentalists and the unconcerned each accounting for roughly 25% of survey populations, while the remaining 50% fell into the middle, privacy pragmatist, group (Kumaraguru and Cranor, 2005). Figure 5 suggests an exponential distribution to privacy concern among the study population. Such a distribution may cause the ordinary least squares method of analysis, the method used in this study, to be dominated by the correlations that exist among the higher levels of measured privacy concern as a result of the lack of observations among the lower levels of privacy concern.

The precise source for the resulting distribution of measured concerns is difficult to determine, and is likely the result of several factors. One factor may be that the true distribution of privacy concerns among the target population of college students may in fact be a long tail distribution, with the bulk of students having high levels of concern for their privacy. This distribution would certainly mirror the findings of literature previously cited, which indicate that Americans in general have a high level of concern for their privacy and which challenges the concern distributions that Westin found. A related factor contributing to this distribution maybe the survey instrument itself as employed in this study. The use of a subset of Smith, Milberg, and Burke's privacy concern questions may not provide a wide enough range of concern levels to be of use to a regression analysis. Self-selection bias, discussed in detail below, is surely another factor, as it is likely that individuals who have high levels of concern for privacy are more likely to participate in a study concerning privacy.

A final potential source of the observed behavior may be that it is reflecting an actual phenomenon. If this is the case, then there are two possible relationships between this phenomenon and the literature; either this phenomenon is described in literature that was not included in the present review, or this observation is new. In the case of the former, this indicates that the literature review may not have been exhaustive enough to create a correct model for hypothesis testing regarding privacy concern and trust. In the case of the latter, the findings of this study regarding privacy concern and trust are suggestive, but not conclusive. In this case, the study would need to be conducted again, perhaps with a modified questionnaire that would provide a clearer picture of the measurement of and relationship between privacy concern and trust.

Self Selection Bias

In any study in which respondents decide whether or not they will participate in the study, including this study, there will be self-selection or non-response bias (Alreck and Settle, 2004). The focus of the present study, privacy, surely influenced the likelihood that a given participant would decide to respond to survey requests. In general, one would expect a high level of concern for privacy to have a negative effect on the likelihood of an individual to respond to a survey of any type. However, the distribution of measured privacy concerns displayed in Figure 5 does not support this expectation. The observed distribution of privacy concern maybe due in part to the IRB requirements of studies involving human subjects which mandate informed consent among respondents of the data that will be collected about them and to what uses it will be placed. Aside from promising potential respondents that personal information would not be collected about them, the informed consent notice also stated that information regarding online privacy protection would be provided to respondents following the survey. This information was provided as an incentive for individuals to respond to the survey, out of concern that not enough individuals would respond without such an incentive. However, it is likely that this incentive contributed to a high number of highly concerned individuals responding to the survey, resulting in the distribution of privacy concern levels observed in Figure 5.

In many instances, self-selection bias can be corrected for to some extent, if there is reason to believe that a given variable impacts the selection decision of participants. By regressing the suspect variable on other variables which may predict the suspect variable, an estimated coefficient for self-selection can be derived and used to correct for self-selection bias in a regression (Heckman, 1979). In this case, a suspect variable exists – privacy concern.

Unfortunately, predictor variables for privacy concern, which would include previous privacy violations (Awad, 2006), perceived risk (Dinev, 2006), and online experience (Jensen, Potts, and Jensen, 2005), do not exist among the collected data. Therefore, this mathematical technique for correcting self-selection bias cannot be used on the collected data.

Omitted Variables

Any social science study is likely to omit variables, given that the total set of all variables present in a situation is simply too large to fully cover and may be unknown at the outset of a study. Omitted variables can result in biases in the coefficients calculated for those variables included in a regression, which can result in significant, unexpected signs on included variables (another potential factor leading to the behavior of privacy concern observed in this analysis.) Omitted variables can also result in poor fits between regression equations and collected data (Studenmund, 2006), a phenomenon that can be seen in the lack of joint-significance for equations in several situations. This phenomenon can also be seen in the very low R^2 values reported for nearly all regressions performed[10].

The literature suggests a number of potential candidate variables that were omitted from this study. Swift discussed the concept that trust actually involves two distinct variables, a measure for the level of trust an individual has for a party and a measure for the level of distrust that individual has for a party. In Swift's model, trust and distrust exist as separate continuums instead of being opposite ends of the same continuum. Yet these two variables continue to have opposing influences in relation to some third measure (corporate accountability in Swift's case) (Swift, 2001). Thus, a lack of a survey instrument for measuring distrust as a distinct variable

[10] R^2 values represent the fit between a regression equation and the data used during analysis, with R^2 = 1 reflecting a perfect fit and R^2 = 0 reflecting a complete lack of fit.

may constitute the omission of a relevant variable, though it is not entirely clear what distrust's role would be in this analysis.

Relying on models for general trust, McKnight developed a model for trust in e-commerce that suggests a pair of omitted variable candidates. *Disposition to Trust*, or the general likelihood that an individual will trust other parties in any circumstance, appears likely to have a positive impact on trust of specific parties in specific situations. Likewise, *Institution-based Trust*, or the trust that an individual has in the environment in which they are operating (the Internet in both this and McKnight's cases) also appears likely to have a positive impact on trust (McKnight, Choudhury, and Kacmar, 2002). While a limited measure for privacy concern was included in the questionnaire, which may be suggestive of disposition to trust and institution-based trust, it is not a direct measure of either, or the related factor of risk tolerance. This is because privacy concern can be informed by multiple factors, which include disposition to trust and institution-based trust, but can also include the personal valuation of privacy and an individual's understanding of what privacy is. Also, the privacy concern questions as used may conflate the disposition to trust and institution-based trust measures.

Skills and history with the Internet are likely to be additional important variables omitted from this study. The Internet skills that an individual has, including both technical skills (such as knowing how to use a browser or a search engine) and "street's smart" knowledge of the Internet (being able to identify scams, phishing attempts, or unreputable websites) may impact both an individual's ability to assess the trustworthiness of parties or facts found on the Internet and an individual's confidence in his/her ability to assess trustworthiness (Hargittai, et al., 2010). As discussed above, previous violations or privacy and Internet experience may contribute to concern for privacy. In addition, these two may also impact trust by increasing or decreasing the amount of trust an individual has for parties online.

Testing Trust without Reputation

The subject of this study was trust in general groups regarding privacy; whether first parties are trusted more than third parties to assist individuals with privacy, and whether government agencies are trusted to oversee privacy aids. Such a focus meant that the study had to be designed so that the history or reputation of specific organizations did not influence, or potentially overshadow, the levels of trust that were measured for the more general categories of organization. Thus, in order to minimize the potential impact of reputations among the public of specific parties, names of actual organizations were not used in the questionnaire.

Tadelis suggests that this is a sound method of testing public trust of a group. All things being equal, and absent information regarding a specific party, if a party is a member of a given group it will inherit the reputation among the public of that group, until the public gains more information and history specific to that party (Tadelis, 2003). Thus, by removing other sources of information or history, the study was able to measure the level of trust the sample population has for the groups in question via the trust that the vaguely described parties in the questionnaire had inherited.

That said, trust in a party is often earned, and levels of trust depend in large part on the history an individual has with that party, or absent personal history, the reputation that party has with the public. The lack of a specific history or reputation from which to draw upon removed a major source of information needed by individuals to make assessments of trust. Thus, the use of vague descriptions for the authoring organizations likely reduced the trust that users had for those organizations, or reduced the occurrence of either very low or very high levels of trust as respondents may have been hesitant to indicate either extreme with little direct information about the organization available (Earp, et al., 2005) (Hargittai, et al., 2010). This may explain the joint insignificance of the constructed equations for the integrity component. Respondents may have been able to glean information regarding the benevolence of the summary author by the fact that the organization wrote a summary at all, or by the content of the summary in the case of first party authors. Furthermore, respondents may have inferred the ability of the summary author to correctly represent the base privacy policy in the created summary simply by the structure of the summary, word use, or the realistic content of the summary. However, in the case of integrity, there are few cues to indicate whether the summary author adheres to any set of values, or that those values would match the values of the respondents.

Contingent Valuation

Contingent valuations involves a distinct set of biases in addition to the biases often found in survey studies. For example, the payment card elicitation method used in this study is known to induce a range bias, in which the range of values presented to the respondent impacts the respondent’s valuation by unintentionally communicating expected values or constraints on reasonable values to the respondent. Scenario and context misspecification biases can also occur based on the wording of questions and statements (Mitchell and Carson, 1989). For example, the use of a yes or no willingness to pay question as the first step in the contingent valuation of this study may have biased responses by unintentionally encouraging respondents to state no willingness to pay instead of a low valuation. In addition, the specification of the good in question, access to the summary of a privacy policy of one website, may have been unclear. Furthermore, it is likely that a different specification of the good in question, such as access to the summary of every website's privacy policy or some other type of access to a privacy information aid, would have been a better subject of the contingent valuation questions.

Given the overwhelming percentage of respondents who did not feel that summaries should have to be paid for, one must raise the question of whether or not contingent valuation is the appropriate method of answering the question of interest – how should providers of privacy information aids be funded? It has been noted that contingent valuation may not be suitable for "small ticket items" which would cost the respondent little, since these small values may not motivate the respondent to consider the true value of the item (Mitchell and Carson, 1989). In addition, the very question of valuing an information aid assumes that respondents lack information relevant to the topic of the question, which may reduce respondents' ability to state a valuation.

Chapter 6 - Discussion

The final chapter of this paper will discuss implications resulting from the earlier literature review, policy analysis, and conducted study. First among these implications will be a discussion of future directions for research in the realm of trust and online privacy. Following this will be a discussion of what this paper's review, analysis, and study reflect about current and future federal policy regarding online privacy. This discussion will include a summarization of observed requirements, constraints, and opportunities for federal policy, and will close with descriptions of three policy alternatives that each address these observed characteristics in part.

Future Research

The limitations of this study discussed above suggest a number of directions for future research. One such direction is to address this study's methodological issues – omitted variables and self-selection bias. A follow up to this study could include survey questions that measure the omitted variables of distrust, disposition to trust, institution-based trust, Internet skills, and online history, and privacy history. Including these variables would require a further review of literature regarding these variables, and may require the formation of new questions for measuring these variables. In addition, a second execution of this study could account for self selection bias, either by including variables predictive of privacy concern or by distributing the survey in a manner that would encourage a greater and more representative response, such as in a class setting (boyd and Hargittai, 2010).

A related question for a follow up study concerns the target population. Due to resource constraints, this study targeted a convenience population of college students. However, as pointed out by (Gachter, Herrmann, and Thöni, 2004), levels of trust can vary across age and socio-economic groups. There certainly is value in studying the influencers of trust of college students regarding online privacy, given the prevalence of both college students and young adults online. However, targeting a wider audience in a future study is clearly important, given that important differences may exist between college students and other groups regarding trust and its influences.

Another direction for future research is to expand the variable of information aid provider to include actual organizations. As discussed, the use of vague descriptions for provider organizations was used to remove the impact of reputations, which is a valid method for measuring the trust of groups but may well impact the levels of trust measured. A modified version of this study could test the trust of actual organizations, making the results of the modified study more concrete and reflective of the current online environment. Furthermore, the modified study could also measure the trust of organizations from different sectors. Based on literature, this study assumed that trust would be greatest for a third party information aid provider that was an educational institution. However, a study of trust by sector regarding information aids may yield different results. In the case of a modified study that measured both the trust of actual organizations and trust across sectors, it would be important to have several organizations representing each sector, so that sector averages could be compared and organizations which elicit an extreme trust or lack of trust do not bias the results.

Finally, with regards to the question of funding information aid providers, the contingent valuation performed in this study was likely premature. Further research and analysis of the needs of information aid providers has to occur before the question of funding can be addressed. The scope of provision – i.e. which websites the providers would target –

would need to be defined, which would require research and analysis of the needs and behaviors of consumers and websites. A question that is actively being researched is how best to construct information aids – the answer to which could ultimately impact the financial needs of information aid providers. These points and others would inform the question that must be addressed before asking about funding: how much does providing information aids cost? Once this question is addressed, then the question of how to fund providers can be pursued more concretely. Finally, when it comes time to address the question of funding, the findings of the contingent valuation performed here provides one conclusion: funding information aid providers by direct consumer contributions is not the best option given the high percentage of individuals who feel they should not have to pay for such a service. However, there are a number of other funding options available, including allocation of government funds or institution of a tax or fee on consumer facing websites, which could be considered based on factors such as political feasibility and available or expected revenue.

Discussion of Findings on Policy

Due to the largely inconclusive nature of the study, the following analysis is pursued with caution, and will focus largely on the few, relatively conclusive findings that emerged. The reader is asked to consider this analysis with the same level of caution and to understand that a future study may yield different findings that will have different implications for policy. That said, it is still valuable to discuss implications in the event that the findings of this study are in fact true. Furthermore, the findings of this study concerning first vs. third party trust are conclusive enough that the author feels comfortable discussing its implications for policy with a high degree of confidence.

This study's chief finding is of a statistically significant difference between the trust individuals place in first party and third party providers of privacy information aids, with third parties being seen as the more trustworthy group by individuals regarding privacy assistance. As indicated by literature, individuals are less likely to consider information or make use of services from parties that they trust less, which means this finding suggests that privacy information aids provided by websites themselves are less likely to be used by individuals than information aids provided by a third party. In reference to the concerns that prompted the policy question of this paper and this study, this finding suggests that a policy which assigns [or assumes] the role of privacy information aid provider to websites will lead to a less than optimal solution to the bounded rationality and information asymmetry problems currently present in the online privacy environment. Such an assignment or assumption will lead to an allocation of resources to parties who, due to lower public trust, are less able to provide assistance to individuals. Ultimately, such a policy will be less successful than a policy which assigns or assumes the same role to third parties when judged by the metric described in the first chapter of this paper: the ability of the policy to provide individuals with useful tools or information that empowers individuals to protect their online information privacy.

The FTC's recently published report asks website operators to assist users in their control of privacy. Federal policy for the previous decade and a half has relied on industry self-regulation based on the actions that website operators should take to assist individuals to control their online privacy. This study's finding regarding first and third party trust indicates a potential weakness in the federal government's historic policy for online privacy and its current approach to policy evolution. The same finding also suggests an obvious alternative policy direction to consider; assign the role of online privacy assistor for individuals to third parties, and pursue policy options that strength the ability of third parties to assist individuals to control their privacy.

Unfortunately, the history of TRUSTe, discussed in the first chapter, demonstrates potential difficulties with a policy that entrusts assistance of individuals to a third party. Third parties may ultimately fail to help individuals and may actually hurt the ability of individuals to control their privacy due to poor service provision or industry pressure. Pressure from industry can have an impact similar to what is seen in regulatory capture – the scenario in which a government agency responsible for regulating a set of entities undertakes actions that favor the ends of the regulated entities at the expense of larger social goals, due to a concentration of influence on the agency from the regulated organizations that is not balanced by the influence of a generally less informed or concerned public (Amann, 2006, pg. 14). TRUSTe would seem to be an ideal example of an organization to entrust with the responsibility of assisting individuals with online privacy. Unlike industry self-regulatory programs managed by industry groups, TRUSTe was not associated with a web business or an industry group. Quite the opposite, TRUSTe was co-founded by the sitting executive director of the EFF (Jennings and Fena, 2000), a non-profit online consumer and individual rights advocacy organization. While industry self-regulation groups are motivated by a need to meet government and consumer demands, TRUSTe appeared to be motivated by a more altruistic desire to help individuals safely interact with the online environment. Yet TRUSTe ultimately fell short of its goal to serve as an independent consumer watchdog. The organization was found to not be performing the auditing functions it claimed to be, gave up on publically reporting consumer complaints about websites (Hirsch, 2010), and its trustmark program was accused of leading to website data practices that were even more threatening of privacy than the average website (Jensen and Potts, 2003) (Edelman, 2011).

While TRUSTe's primary function was and is monitoring compliance of websites with its own standard of privacy practices, its history can be an informative and cautionary tale for the consideration of policy that entrusts the role of consumer assistor to a third party. This is true at least in part because TRUSTe's primary means of compliance enforcement was by publicizing information, a function similar to what is being discussed in this paper for privacy information aid providers. A full analysis of why TRUSTe could not meet its goals was not conducted for this paper, but a couple of factors can be discussed here. TRUSTe's practice of granting privacy seals despite not actually performing audits, and the end of its public reporting of complaints, point to a need for a third party assistor to be transparent in its processes and accountable to some other party. In addition, the end of TRUSTe's public reporting of complaints, its restructuring from a non-profit to a for-profit organization (Weisenthal, 2008), and its lack of performing audits, all point to potential problems in TRUSTe's funding model. TRUSTe' may not have been receiving the financial resources necessary to perform all of the functions that it wished to. Furthermore, its model of charging website operators to display its voluntary privacy seal may have introduced a conflict of interest, since TRUSTe had an economic incentive to increase the number of websites that were displaying its seal.

Another finding from the performed study, if it is true, suggests that government involvement in overseeing provision of privacy aid has no impact on the trust that individuals place in the provider of aid. This means that the government cannot build public trust for a given provider of privacy aid, at least not via oversight. However, this also suggests that government oversight does not diminish the trust that the public has for a provider of privacy aid. Thus, a federal agency appears to be free to provide oversight in the provision of privacy information aids, if need be, without fear of negatively impacting the ability (with regard to trust) of the privacy information aid provider to provide its information and services. Such flexibility means that a federal agency may be able to address the two issues raised by TRUSTe's history cited above. By doing so, a federal agency may be able to strength a policy option which entrusts third parties to provide privacy information aids to consumers.

Policy Alternatives

Having considered the results of the present study, the analysis of current federal policy, and the identification of needs, I would like to conclude this paper by describing three policy alternatives to be considered by federal policy makers – in particular those in the FTC and representatives in Congress. These three alternatives; modifying and adopting the recently introduced Commercial Privacy Bill of Rights Act, encouraging research and development of privacy information aids, and encouraging the growth of a market of privacy information aid providers; are chosen for consideration because they target one or more of the identified requirements and satisfy identified constraints. Before discussing the policy alternatives, identified requirements and constraints will be summarized.

Identified Requirements, Constraints, and Opportunities

Through a literature review, policy analysis, and a scientific study, this paper demonstrates a number of requirements, constraints, and opportunities for federal policy regarding online privacy. In this discussion, a requirement refers to some goal that a policy alternative should attempt to reach; a constraint refers to some limitation that prevents certain actions, and an opportunity refers to some freedom of action available to policy makers or implementers. Identified requirements, constraints, and flexibilities are summarized in Table 16 so as to inform the policy alternatives that follow.

Requirements	
Socially Dynamic Definition of Privacy	American society has not yet defined what privacy means in the current age nor has it conclusively ranked the value of privacy compared to other competing values. Policy alternatives should seek to leave definition of privacy and relative value ranking up to a social discussion, or at least a discussion involving many relevant stakeholders. Policy alternatives should seek to provide information to assist the social or stakeholder discussions.
Enforcement and Accountability	Current self regulation provides little in the way of enforcing established principles, making those principles hollow and poor tools for enabling individuals to control their privacy. History shows that even well intentioned organizations need to be accountable to some other party to avoid various influences or natural tendencies. Policy alternatives should seek to provide increased enforcement abilities and means for overseeing the actions of privacy assisting organizations.
Address Information Asymmetry and Bounded Rationality	Individuals currently do not have access to all information needed to make decisions regarding control of privacy, or are in other ways constrained in their ability to make privacy decisions. These current limitations may also negatively impact the ability of individuals to participate in the process of socially defining privacy and its relative value. Policy alternatives should seek to develop technical, social, and/or economic tools that increase individuals' access to information and ability to utilize that information.
Financial support	Implementation of any policy requires a consistent source of revenue to fund policy actions. Policy alternatives should consider how to finance the agency/organization that will implement policy.
Constraints	
Website Operator Trust	Individuals are less trusting of attempts by website operators to provide privacy information aids. Policy alternatives cannot assume or rely on website operators to perform actions that provide privacy assisting information or tools to individuals.
Consumers Will Not Pay For Assistance	Although individuals feel that privacy information aids should be provided to them, a vast majority of individuals do not think they should have to pay for these tools or information. Policy alternatives cannot rely on Internet users as a direct source of revenue for policy implementation.
Voluntary Fees Create a Conflict of	Voluntary payments from website operators to third parties create an economic incentive for the third parties to provide individuals

Interest	with information or tools that portray the website in a positive light. Policy alternatives cannot rely on voluntary payments from website operators as a source of revenue for policy implementation.
Opportunities	
Federal Involvement	Federal involvement in the provision of privacy assisting information or tools does not appear to positively or negatively impact the trust of individuals for the information or tool. Involvement of federal agencies is an option available in the creation or execution of policy alternatives.

Table 16 - Requirements, Constraints, and Opportunities for Policy Alternatives

Modify and Adopt the Commercial Privacy Bill of Rights Act

The Commercial Privacy Bill of Rights Act of 2011 (Kerry and McCain, 2011), also known as S. 799, was introduced into the United States Senate earlier this year by Senators Kerry and McCain with the intent of increasing privacy protection among individual Americans from private commercial organizations by increasing the FTC's authority regarding online privacy. S. 799 does this by mandating the FTC to initiate a number of rule making processes that address components of the FIPP, the OBA self-regulatory principles, and the most recently published FTC report on consumer Internet privacy. Relevant to this analysis, the act mandates that the FTC initiate a rule making process for commercial organizations to clearly notify individuals of their data practices and changes to those practices. The FTC is also allowed to bring enforcement actions under the act against organizations that collect or share consumer information that have violated the rules or requirements of the act.

In addition to enhanced enforcement capabilities and rule making responsibilities, S. 799 also describes a safe harbor program that the FTC will be responsible for and maintain oversight over. Nongovernmental organizations would be allowed to operate privacy programs which website operators could choose to participate in. By participating in a program, website operators would no longer be directly liable under several of S. 799's requirements. However, these programs would be required to implement the requirements of S. 799 and the FTC rules that are created as a result of it among participating commercial organizations. The FTC would exercise oversight by selecting the nongovernmental organizations that can operate as official safe-harbor program administrators, and by performing audits of a safe-harbor program's adherence to S. 799. Those programs found to not be complying with the act could face penalties or could have their safe-harbor authorization revoked, which would expose the website operators who participate in the program to liability under the act.

S. 799, as it currently exists, addresses the enforcement and accountability need identified earlier by providing the FTC with direct legal authority over online privacy protection though both direct enforcement and oversight of safe harbors. By enhancing enforcement while still maintain a flexible rule making process, which in the FTC's history often includes input from several stakeholders including industry and consumers, the act also maintains some of the socially defined nature of privacy offered by the flexibility of the current self-regulatory definition of rules. The act, however, does not provide a novel approach to the information asymmetry and bounded rationality problems – the act's treatment of this issue is largely the status quo of instructing the FTC to guide industry in its attempts to provide consumers with information and choice.

Based on the findings of the present study, I suggest that two amendments be made to S. 799. The first addresses the rule making mandated by the act. The rule making regarding the clear description of data practices by website operators should be modified to be a rule making that requires website operators to seek out a third party to provide the clear description of data practices to consumers. This same rule may also create requirements for the third parties as to what the clear description of data practices must include, just as the rule making process as currently described by the act does for first parties. The amended rule should be technologically agnostic like the currently described rule making process. The second amendment is a corollary of the first, applied to the safe harbor portion of the act. Under this amendment, rule making for the safe harbor program would require that safe harbor administrating organizations either provide third party privacy information aids themselves to individuals who use the websites of participating organizations, or require the safe harbor program to contract with some other third party for the provision of privacy information aids. Both amendments should also provide the FTC with some level of oversight over the third parties providing privacy information aids so as to make the third party privacy information aid providers accountable to some other party. This oversight may include regularly scheduled audits or reporting requirements of the information aid providers, as well as empowering the FTC to levy fines or revoke the ability of an organization to provide privacy information aids if an organization is found to not be complying with the rules created by the FTC's rule making process or the act.

If amended as above, S. 799 would address the information asymmetry and bounded rationality problems while respecting the constraint that providers of information aids to consumers should not be website operators. As a whole, the amended S. 799 would employ the available opportunity of federal involvement in online privacy to address all of the requirements of federal policy except for financing its execution.

Encourage Research and Development of Privacy Information Aids

This alternative and the final alternative concern the general stance of the FTC on a policy matter. They may require actions that cannot currently be taken by the FTC and are not currently being considered by Congress. Thus, these alternatives encourage the FTC to work with other agencies on executing a policy and being supportive of actions that can be taken by others.

The present alternative is for the FTC to be supportive of efforts to research and develop privacy information aids by academia and the private sector. This policy seeks to encourage the type of research performed by (Vail, Earp, and Anton, 2008) and (Masson and Waldron, 1994) so as to produce privacy information aids that effectively provide individuals with the information needed to control their privacy and address the information asymmetry and bounded rationality issues currently present. As indicated by the results of the present study, this policy should specifically encourage organizations that are not currently operators of websites that provide consumer content or services, as issues of public trust may inhibit the effectiveness of privacy information aids researched and developed by organizations which focus on consumer content or services.

Encouragement in this alternative has two potential components: constructive guidance of research and development, and financial support. Constructive guidance entails the FTC providing information to researchers and developers about what, in its view, privacy information aids need to provide and how they may be designed. The FTC may posit research questions or ideas for research agendas to academia and the private sector, informed by the FTC’s unique role as a solicitor of input from multiple stakeholders. In light of the FTC’s history of report publication, this component of support is very similar to the FTC’s current practices, and should be quite easy to implement.

The second component of encouragement, financial support, is more difficult. The FTC is not a funding agency. Creating a research and development fund administered by the FTC, using fees levied as a result of Section 5 FTC enforcement actions, is a potential action the commission can undertake to directly provide financial support to academia and industry. However, the commission will likely need to work with the traditional research funding agencies, such as the National Science Foundation and the National Institutes of Health, and advocate that these agencies provide funding to support the research and development efforts of academics and members of the private sector who are working towards useful privacy information aids.

Unlike the first alternative, this alternative attempts to address, in part, the issue of financing its own implementation while respecting the financing constraints identified. Information asymmetry and bounded are also addressed, and privacy is still left to be social defined. However, this alternative does not take advantage of the opportunity for federal involvement to increase enforcement or accountability among website operators or information aid providers.

Encourage Growth of Market of Privacy Information Aid Providers

The final alternative to be discussed in this paper maybe the most difficult for the FTC to implement, and likely requires further development before being implemented. This alternative seeks to address the financial issues of operating an organization that provides privacy information aids to consumers. As illustrated by TRUSTe, this issue is important to consider, as problems resulting from a lack of financial resources or the source of those resources may greatly undermine the ability of an organization to effectively provide services that inform consumers about commercial organizations.

As with the encouraging research and development alternative, this alternative would involve two components of encouragement: providing information and providing financial resources. Publication of information may be as simple as the FTC publicizing its desire and administrative support for organizations that act as third party privacy information aid providers. The commission may also create guiding documents similar to the FIPP, which describe its vision of what an effective third party provider of privacy information aids would seek to accomplish. The commission could also act in its traditional role as a solicitor and mediator of stakeholder opinions that can inform the operation of third party privacy information aid providers.

Again, the FTC is unlikely to be able to provide financial resources to organizations wishing to participate in a market of privacy information aid providers. However, the FTC may act as a match maker, informing organizations that would like to become privacy information aid providers of agencies or foundations that are potential sources of financial resources. As the financial needs of third party privacy information aid providers become more clear overtime, the FTC may also attempt to develop and lobby for revenue models for third party privacy information aid providers. Findings of the present study suggest that relying on direct consumer payments may not be a successful model, and the history of TRUSTe shows that a model of voluntary payments from websites may create a conflict of interest. However, other revenue models exist for consideration, some of which may include government involvement. Such models include revenue coming primarily from federal sources, such as Congressional or agency appropriations; or revenue that is funded by a tax levied on organizations which collect, store, process, or share information about consumers.

Like the previous alternative, this alternative focuses on part of the requirement of financing policy execution. This alternative also addresses information asymmetry and bounded rationality, like the previous alternative, as well as allows for a socially dynamic definition of privacy. However, like the previous alternative, enforcement and accountability are not increased under this alternative.

Chapter 7 - Conclusion

This thesis has examined the online privacy environment of individuals in relation to private organizations through an analysis of federal policy regarding individual privacy and a scientific study of the trust and valuation that individuals place in those who attempt to aid their online privacy. Policy analysis found a weakness in current policy – namely the ineffectiveness of current policy to provide individuals with relevant information – that significantly hinder the current policy's ability to meet its goals of protecting the privacy-related self-interests of individuals and providing a mechanism by which the socially dynamic nature of privacy can fairly evolve. This same analysis also found strengths, namely the ability of the policy to increase the presence of privacy policies online and the flexibility the policy provides for the setting of rules and establishment of the social value of privacy. A scientific survey yielded three findings: individuals in college trust privacy information aid providers more as third parties in an online interaction than as the website within which they are primarily interacting; the trust of individuals in college for information aid providers is not significantly impacted by the involvement of federal oversight; and individuals in college are not willing to directly pay for information aids.

The results of this analysis and study lead me to suggest a policy direction. In lieu of the implementation of an entirely new policy, I've argued that the weakness of the current policy should be addressed so that our nation can continue to benefit from the strengths of the current policy at a time when they are still needed. One method for addressing this weakness, discussed elsewhere and focused on here, is to increase the availability of privacy information aids that assist individuals in understanding the online privacy environment and making informed decisions. With trust as the primary metric, the present study suggests that third party organizations should be the primary provider of these privacy information aids instead of first party websites, which is what historic and current policy has assumed. In addition, the present study suggests that, based on the metric of trust, the federal government is free to involve itself in the third party provision of information aids – which maybe necessarily given the history of similar initiatives – without significantly impacting the trust that individuals place in third party information aid providers. Finally, the present study indicates that consumers are unwilling to pay for privacy information aids, showing that neither policy makers nor information aid providers can rely on direct payments from individuals to fund privacy information aid provision.

Three potential policy alternatives were discussed for increasing the availability of privacy information aids. These alternatives take into account the findings of the present study while attempting to address how best to promote the development and deployment of privacy information aids. The discussion of these alternatives here is a first step, and further development of these alternatives is required before they are ready for implementation. Regardless of the maturity or merits of the alternatives discussed in this paper, the analysis and findings presented here have demonstrated that discussions of federal policy regarding the online privacy of individuals from private organizations need to include considerations of how information is provided to individuals in addition to what information should be provided. Simply making information accessible to individuals is not enough to make it useful; assistance and capabilities must also be present.

Bibliography

Acquisti, A., and J. Grossklags. "Privacy and Rationality in Individual Decision Making." *Security & Privacy, IEEE* 3.1 (2005): 26-33. Web.

Albanesius, Chloe. "Apple Adds 'Do Not Track' Option to Safari." PC Mag.com. 4/14/2011. Web. 4/15/2011. <http://www.pcmag.com/article2/0,2817,2383565,00.asp>.

Alexa. "Eharmony.com Site Info." 2011. Web. 3/11/2011 <http://www.alexa.com/siteinfo/eharmony.com>.

---. "Match.com Site Info." 2011. Web. 03/11/2011. <http://www.alexa.com/siteinfo/match.com>.

---. "Zoosk.com Site Info." 2011. Web. 3/11/2011 <http://www.alexa.com/siteinfo/zoosk.com>.

Alreck, Pamela L., and Robert B. Settle. *The Survey Research Handbook*. 3rd ed. Boston: McGraw-Hill Irwin, 2004. Print.

Amann, Edmund. *Regulating development: evidence from Africa and Latin America*. Northampton, MA: Edward Elgar Publishing, 2006.

American Association of Advertising Agencies, et al. *Self-Regulatory Principles for Online Behavioral Advertising*., 2009. Web. 4/29/2011. < http://www.the-dma.org/government/ven-principles%2007-01-09%20FINAL.pdf>.

Anton, Annie I., and Julia B. Earp. "A Requirements Taxonomy for Reducing Web Site Privacy Vulnerabilities." *Requirements engineering* 9.3 (2004): 169. Web. 2/10/2011.

Anton, Annie I., Julia B. Earp, and Jessica D. Young. "How Internet Users' Privacy Concerns have Evolved since 2002." *Ieee Security & Privacy* 8.1 (2010): 21-7. Web.

Armbrust, Michael, et al. *Above the Clouds: A Berkeley View of Cloud Computing*. UCB/EECS-2009-28 Vol. Berkeley, CA: Electrical Engineering and Computer Sciences - University of California at Berkeley, 2009. Web. 6/30/2010. < http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>.

Arrington, Mike. *Mark Zuckerberg at Crunchies.* ustream.tv, 1/2010. Web. 2/7/2011. < http://vodpod.com/watch/2839774-mark-zuckerberg-at-crunchies>.

Assessment of Demand Response and Advanced Metering. Federal Energy Regulatory Commission, 2011. Web. 4/11/2011. < http://www.ferc.gov/legal/staff-reports/2010-dr-report.pdf>.

Awad, N. F. F. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization." *MIS quarterly* 30.1 (2006): 13-28. Web. 2/1/2011.

Ba, Sulin, and Paul A. Pavlou. "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior." *MIS Quarterly* 26.3 (2002): 243-268. Web.

Beldad, Ardion, Menno de Jong, and Michael Steehouder. "Reading the Least Read? Indicators of Users' Intention to Consult Privacy Statements on Municipal Websites." *Government Information Quarterly* 27.3 (2010): 238-44. Web.

Blind, Peri K. *Building Trust in Government in the Twenty-First Century: Review of Literature and Emerging Issues*. United Nations Department of Economic and Social Affairs, 11/2006. Web. 5/23/2011. < http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN025062.pdf>.

Blumberg, Andrew J., and Peter Eckersley. *On Locational Privacy, and how to Avoid Losing it Forever*. Electronic Frontier Foundation, 8/2009. Web. 4/13/2009. < http://www.eff.org/wp/locational-privacy>.

boyd, danah, and Eszter Hargittai. "Facebook Privacy Settings: Who Cares?" *First Monday* 15.8 (2010) Web. 4/17/2011. < http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589>.

boyd, danah. *Making Sense of Privacy and Publicity*. SXSW: 3/13/2010. Web. 4/10/2010. < http://www.danah.org/papers/talks/2010/SXSW2010.html>.

Bryan, Richard H. *Children's Online Privacy Protection Act of 1998*. Pub. L. 105-277, div. C, title XIII, 105th. 1998.

Cavoukian, Ann. *Operationalizing Privacy by Design:The Ontario Smart Grid Case Study*. 2/02/2011. Web. 2/02/2011. < http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1037>.

Cho, Hichang, Milagros Rivera-Sánchez, and Sun Sun Lim. "A Multinational Study on Online Privacy : Global Concerns and Local Responses." *New media & society* 11.3 (2009): 395-416. Web. 2/1/2011.

Clinton, William J., and Albert Gore. *The Framework for Global Electronic Commerce*. 7/1/1997. Web. 4/21/2011. < http://clinton4.nara.gov/WH/New/Commerce/read.html>.

Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework. Department of Commerce, 12/16/2010. Web. 4/17/2011. < http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf>.

Culnan, Mary J., and Pamela K. Armstrong. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science* 10.1 (1999): 104-115. Web.

Culnan, Mary J. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing." *Journal of Direct Marketing* 9.2 (1995): 10-19. Web.

---. *Privacy and the Top 100 Web Sites: Report to the Federal Trade Commission*. Online Privacy Alliance, 6/1999. Web. 5/3/2011. < http://www.securitymanagement.com/archive/library/elec_privacy.pdf>.

---. "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy & Marketing* 19.1, Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy (2000): 20-26. Web. 2/1/2011.

Dinev, Tamara, and Paul Hart. "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research* 17.1 (2006): 61-80. Web.

Direct Marketing Association. "Complaint Handling Procedures & How To File A Complaint." 2011. Web. 4/29/2011. < http://www.the-dma.org/guidelines/complaintprocedures.shtml>.

---. "DMA Board Approves Online Behavioral Advertising & Mobile Marketing Guidelines for Interactive Marketing." 10/19/2009. Web. 4/29/2011 <http://www.the-dma.org/cgi/disppressrelease?article=1357>.

---. "DMA Online Behavioral Advertising (OBA) Compliance Alert & Guidelines for Interest-Based Advertising." 2009. Web. 4/29/2011. <http://www.dmaresponsibility.org/privacy/oba.shtml>.

---. *Guidelines for Ethical Business Practices*. 2010. Web. 4/29/2011. < http://www.dmaresponsibility.org/Guidelines/>.

Earp, Julia B., et al. "Examining Internet Privacy Policies within the Context of User Privacy Values." *IEEE Transactions on Engineering Management* 52.2 (2005): 227-37. Web.

Edelman, Benjamin. "Adverse Selection in Online “trust” Certifications and Search Results." *Electronic Commerce Research and Applications* 10.1 (2011): 17-25. Web.

Egelman, Serge, et al. "Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators." *Proceedings of the 27th international conference on Human factors in computing systems*, *April 3rd - 9th, 2009.* Boston. Association of Computing Machinery, 2009. Web.

eHarmoney.com. "Company Overview." 2010. Web. 3/11/2011 <http://www.eharmony.com/about/eharmony>.

Electronic Privacy Information Center. "In the Matter of Facebook, Inc." 5/5/2010. Web. 4/9/2011. <http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf>.

Ervin, Sam J., Jr. *Privacy Act of 1974*. Pub. L. 93-579, 93rd. 1974.

Facebook.com. "Controlling How You Share." 2011. Web. 5/4/2011. <https://www.facebook.com/privacy/explanation.php>.

Federal Trade Commission. *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*. 2009. Web. <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

---. *In the Matter of Google Inc.* Federal Trade Commission, 2011. Web. 4/4/2011. < http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf>.

---. *In the Matter of Google Inc. Federal Trade Commission: Agreement Containing Consent Order*. 3/30/2011. Web. 4/10/2011. <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf>.

---. *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*. 12/20/2007. Web. 4/24/2011. < http://www.ftc.gov/os/2007/12/P859900stmt.pdf>.

---. *Privacy Online: A Report to Congress*. 6/1998. Web. 4/18/2011. < http://www.ftc.gov/reports/privacy3/priv-23a.pdf>.

---. *Privacy Online: Fair Information Practices in the Electronic Marketplace - A Report to Congress*. 5/2000. Web. 5/3/2011. < http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

---. *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*. 12/2010. Web. 12/14/2010. < http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

Friedland, Gerald, and Robin Sommer. "Cybercasing the Joint: On the Privacy Implications of Geo-Tagging." 8/2010. Web. 4/12/2011. < http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf>.

Gächter, Simon, Benedikt Herrmann, and Christian Thöni. "Trust, Voluntary Cooperation, and Socio-Economic Background: Survey and Experimental Evidence." *Journal of Economic Behavior & Organization* 55.4 (2004): 505-31. Web.

Gibbs, Jennifer L., Nicole B. Ellison, and Chih-Hui Lai. "First Comes Love, then Comes Google: An Investigation of Uncertainty Reduction Strategies and Self-Disclosure in Online Dating." *Communication Research* 38.1 (2011): 70-100. Web.

Gomez, Joshua, Travis Pinnick, and Ashkan Soltani. *Know Privacy*. University of California Berkeley School of Information, 6/1/2009. Web. 4/10/2011. < http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf>.

Goodwin, Cathy. "Privacy: Recognition of a Consumer Right." *Journal of Public Policy & Marketing* 10.1 (1991): pp. 149-166. Web.

Gramm, Phil, Jim Leach, and Thomas J. Bliley. *Financial Services Modernization Act of 1999*. Pub. L. 106-102, 105th. 1999.

Hann, Il-Horn, et al. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems* 24.2 (2007): 13-42. Web.

Hargittai, Eszter, et al. "Trust Online: Young Adults' Evaluation of Web Content." *International Journal of Communications* 4 (2010): 468-494. Web.

Harris Interactive, Inc. *Privacy Notices Research Final Results*. # 15338. 12/2001. Web. 3/24/2011. < http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf>.

Heckman, James J. "Sample Selection Bias as a Specification Error." *Econometrica* 47.1 (1979): 153-161. Web.

Hirsch, Dennis D. "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" *Seattle University Law Review* 34.2 (2010): 439-80. Web.

Hoffman, Marcia. "Trade Commission Enforcement of Privacy." *Proskauer on Privacy.* Ed. Kristen J. Mathews. 5th ed. New York: Practicing Law Institute, 2011. 1-80. Print.

Hofstede, Geert. *Cultures and Organizations: Software of the Mind*. London: McGraw-Hill, 1991. Print.

Hoofnagle, Chris Jay, and Jennifer King. *Research Report: What Californians Understand about Privacy Offline*. University of California Berkeley School of Law, 5/15/2008. Web. 5/5/2011. < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075>.

Horan, Pam. *Re: FTC Staff Preliminary Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" – File no. P095416*. Ed. Federal Trade Commission. Online Publishers Association, 2011. Web. 3/11/2011. < http://www.ftc.gov/os/comments/privacyreportframework/00315-57664.pdf>.

Horrigan, John B. *Use of Cloud Computing Applications and Services*. Pew Research Center's Internet & American Life Project, 9/12/2008. Web. 3/21/2011. < http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx>.

Jennings, C., and L. Fena. *The Hundredth Window: Protecting Your Privacy and Security in the Age of the Internet*. 1st ed. New York: The Free Press, 2000. Print.

Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior." *International journal of human-computer studies* 63.1-2 (2005): 203-27. Web. 2/2/2011.

Jensen, Carlos, and Colin Potts. "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices." *Proceedings of ACM CHI 2004 Conference on Human Factors in Computing Systems, 471-478.* April 24-29, 2004, Vienna. Association of Computing Machinery. Web.

Jøsang, Audun, Roslan Ismail, and Colin Boyd. "A Survey of Trust and Reputation Systems for Online Service Provision." *Decision Support Systems* 43.2 (2007): 618-44. Web.

Kang, Jerry. "Information Privacy in Cyberspace Transactions." *Stanford Law Review* 50 (1998): 1193-202. Web.

Kastenmeier, Robert W. *Electronic Communications Privacy Act of 1986*. Pub. L. 99-508, 99th. 1986.

Kennedy, Edward, and Nancy Kassebaum. *Health Insurance Portability and Accountability Act of 1996*. Pub. L. 104-191, 104th. 1996.

Keppel, Geoffrey. *Design and Analysis: A Researcher's Handbook*. 2nd ed. Englewood Cliffs, New Jersey: Prentice-Hall, 1982. Print.

Kerry, John, and John McCain. *Commercial Privacy Bill of Rights Act of 2011*. S. 799, 112th. 2011.

Kumaraguru, Ponnurangam, and Lorrie Faith Cranor. *Privacy Indexes: A Survey of Westin's Studies*. CMU-ISRI-5-138 Vol. Software Research International, Carnegie Mellon University, 12/2005. Web. 4/10/2011. < http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf>.

Leibowitz, Jon. *So Private, so Public: Individuals, the Internet & the Paradox of Behavioral Marketing*. 11/1/2007. Web. 5/4/2011. < http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf>.

Lenhart, Amanda, and Mary Madden. *Teens, Privacy and Online Social Networks* . Pew Research Center's Internet & American Life Project, 4/18/2007. Web. 4/6/2011. < http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx>.

Lenhart, Amanda. *Protecting Teens Online*. Pew Research Center's Internet & American Life Project, 3/17/2005. Web. 4/6/2011. < http://www.pewinternet.org/Reports/2005/Protecting-Teens-Online.aspx>.

Lessig, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006. Print.

Liu, Chang, Jack T. Marchewka, and Catherina Ku. *American and Taiwanese Perceptions Concerning Privacy, Trust, and Behavioral Intentions in Electronic Commerce*. 12 Vol. , 2004. Web. 2/04/2011.

Majoras, Deborah Platt. *Remarks of Deborah Platt Majoras to the Anti-Spyware Coalition*. 2/9/2006. Web. 5/4/2011. < http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf>.

Masson, Michael E. J., and Mary Anne Waldron. "Comprehension of Legal Contracts by Non-Experts: Effectiveness of Plain Language Redrafting." *Applied Cognitive Psychology* 8.1 (1994): 67-85. Web.

Match.com. "About Match.com." 2011. Web. 3/11/2011. <http://www.match.com/help/aboutus.aspx>.

---. "Privacy Statement." February 8th, 2011. Web. 3/13/2011 <http://www.match.com/registration/privacystatement.aspx>.

May, Patrick, and Dana Hull. "PG&E unveils 'opt-out' plan for its controversial SmartMeter program." 3/24/2011 2011. Web. <http://www.mercurynews.com/breaking-news/ci_17692729?nclick_check=1>.

Mayer, Roger C., James H. Davis, and F. David Schoorman. "An Integrative Model of Organizational Trust." *The Academy of Management Review* 20.3 (1995): pp. 709-734. Web.

Mayer, Roger C., and James H. Davis. "The Effect of the Performance Appraisal System on Trust for Management: A Field Quasi-Experiment." *Journal of Applied Psychology* 84.1 (1999): 123-36. Web.

McDonald, Aleecia M., and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4.3 (2008): 543-68. Web.

McKnight, D. H., Vivek Choudhury, and Charles Kacmar. "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology." *Information Systems Research* 13.3 (2002): 334-59. Web.

Mendez, Fernando, and Mario Mendez. "Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States." *Publius* 40.4 (2010): 617-45. *CSA Worldwide Political Science Abstracts.* Web.

Milne, George R., and Mary J. Culnan. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or don’t Read) Online Privacy Notices." *Journal of Interactive Marketing* 18.3 (2004): 15-29. Web.

Milne, George R., Andrew J. Rohm, and Shalini Bahl. "Consumers’ Protection of Online Privacy and Identity." *Journal of Consumer Affairs* 38.2 (2004): 217-32. Web.

Mitchell, Robert C., and Richard T. Carson. *Using Surveys to Value Public Goods: The Contingent Valuation Method*. Washington, D.C.: Resources for the Future, 1989. Print.

Moldvay, Caitlin. *Dating Game: With Increasing Internet Penetration, Online Dating is on the Rise*. # 81299a. 12/2010. Web. 3/11/2011. < http://www.ibisworld.com/industryus/default.aspx?indid=1723>.

Moor, J. H. "Towards a Theory of Privacy in the Information Age." *Computers and Society* 27.3 (1997): 27. Web.

Morgeson, Forrest V., David VanAmburg, and Sunil Mithas. "Misplaced Trust? Exploring the Structure of the E-Government-Citizen Trust Relationship." *Journal of Public Administration Research and Theory* 21.2 (2010): 257-83. Web.

Mozilla. "Mozilla Firefox 4 Beta, now including "Do Not Track" capabilities." 2/8/2011. Web. 5/4/2011 <http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/>.

Networking Advertising Initiative. "Opt Out of Behavioral Advertising." 2010.Web. <http://www.networkadvertising.org/managing/opt_out.asp>.

---. "Participating Networks." 2010. Web. 4/29/2011. <http://www.networkadvertising.org/participating/>.

Nye, J. "Introduction: The Decline of Confidence in Government." *Why People Don't Trust Government.* Eds. J. Nye, P. Zelikow, and D. King., 1997. Print.

Office of Institutional Research. "All Enrollment Data for Spring 2011." 5/1/2011. Web. 6/2/2011 <http://www.oir.umn.edu/student/enrollment/term/1113/current/show_all>.

Office of the New York State Attorney General. "TO MARK NATIONAL CONSUMER PROTECTION WEEK, A.G. SCHNEIDERMAN RELEASES NYS TOP TEN FRAUDS OF 2010." 3/6/2011. Web. 4/9/2011. <http://www.ag.ny.gov/media_center/2011/mar/mar6a_11.html>.

O'Neill, Michael. "Public Confidence in Charitable Nonprofits." *Nonprofit and Voluntary Sector Quarterly* 38.2 (2009): 237. Web.

Parent, Michael, Christine A. Vandebeek, and Andrew C. Gemino. "Building Citizen Trust through E-Government." *Government Information Quarterly* 22.4 (2005): 720-36. Web.

Personal Information Protection and Electronic Documents Act. Canada, 2000.

Pew Research Center for the People & the Press, The. *The People and their Government: Distrust, Discontent, Anger and Partisan Rancor*. 4/18/2010. Web. 5/23/2011. < http://people-press.org/files/legacy-pdf/606.pdf>.

Pitkow, Jim, and Colleen Kehoe. "GVU's 5th WWW User Survey." 1996.Web. 4/9/2011. <http://www.cc.gatech.edu/gvu/user_surveys/survey-04-1996/>.

Post, Robert C. "The Social Foundations of Privacy: Community and Self in the Common Law Tort." *California Law Review* 77.5 (1989): 957-1010. Web.

Prosser, William L. "The Uncertain Protection of Privacy by the Supreme Court." *California Law Review* 48.3 (1960): 383-423. Print.

Raphael, JR. "Facebook Privacy Change Sparks Federal Complaint." *ABC News*. 2/18/2009. Web. <http://abcnews.go.com/Technology/PCWorld/story?id=6900228>.

Rasmusson, Lars, and Sverker Jansson. "Simulated Social Control for Secure Internet Commerce." *Proceedings of the 1996 New Security Paradigms Workshop,* 18-25. Association for Computing Machinery. 1996. Web. 3/15/2011.

Rifon, Nora J., Robert LaRose, and Sejung Marina Choi. "Your Privacy is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures." *Journal of Consumer Affairs* 39.2 (2005): 339-62. Web.

Rose, E. A. "An Examination of the Concern for Information Privacy in the New Zealand Regulatory Context." *Information & Management* 43.3 (2006): 322-35. Web. 1/27/2011.

Schlosser, Ann E., Tiffany Barnett White, and Susan M. Lloyd. "Converting Web Site Visitors into Buyers: How Web Site Investment Increases Consumer Trusting Beliefs and Online Purchase Intentions." *Journal of Marketing* 70.2 (2006): 133-48. Web.

Schwaig, Stewart K. "Compliance to the Fair Information Practices: How are the Fortune 500 Handling Online Privacy Disclosures?" *Information & management* 43.7 (2006): 805-20. Web. 2/2/2011.

Slutsky, Irina. "Get Hooked Up with the Big Business of Online Dating." *Advertising Age* 82.7 (2011): 32. Web.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly* 20.2 (1996): 167-196. Web.

Smyth, Barry. "ADAPTIVE INFORMATION ACCESS: PERSONALIZATION AND PRIVACY." *International Journal of Pattern Recognition and Artificial Intelligence* 21.2 (2007): 183. Web. 2/1/2011.

Solove, Daniel J. *Understand Privacy*. Cambridge: Harvard University Press, 2008. Print.

Sprenger, Polly. "Sun on Privacy: 'Get Over it'." *Wired*. 1/26/1999. Web. 3/17/2011. < http://www.wired.com/politics/law/news/1999/01/17538>.

Strickling, Lawrence E. *Testimony of Lawrence E. Strickling*. Tran. United States Senate. 3/16/2011. Web. 4/17/2011. < http://www.ntia.doc.gov/presentations/2011/Strickling_Senate_Privacy_Testimony_03162011.pdf>.

Studenmund, A. H. *Using Econometrics: A Practical Guide*. 5th ed. Boston: Pearson Education, Inc., 2006. Print.

Swift, Tracey. "Trust, Reputation and Corporate Accountability to Stakeholders." *Business Ethics: A European Review* 10.1 (2001): 16-26. Web.

Tadelis, Steven. "Firm Reputation with Hidden Information." *Economic Theory* 21.2 (2003): 635-51. Web. 3/15/2011.

Tsai, Janice Y., et al. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research, Articles in Advance* (2009) Web. 3/11/2011.

Turow, Joseph, Lauren Feldman, and Kimberly Meltzer. *Open to Exploitation: American Shoppers Online and Offline*. Annenberg Public Policy Center of the University of Pennsylvania, 6/2005. Web. 4/22/2011. < http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>.

Turow, Joseph. *Americans and Online Privacy - the System is Broken*. Annenberg Public Policy Center of the University of Pennsylvania, 6/2003. Web. 4/22/2011. < http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=36>.

Turow, J. "Internet Privacy and Institutional Trust: Insights from a National Survey." *New media & society* 9.2 (2007): 300-18. Web. 2/2/2011.

Vail, Matthew W., Julia B. Earp, and Anni I. Anton. "An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies." *IEEE Transactions on Engineering Management* 55.3 (2008): 442-54. Web. 2/10/2011.

Waldman, Steven. *The Information Needs of Communities: The Changing Media Landscape in a Broadband Age*. Federal Communications Commission, 6/2011. Web. 6/24/2011. < http://www.fcc.gov/infoneedsreport>.

Warren, Samuel V., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4.5 (1890): 193-220. Web.

Weisenthal, J. "Privacy Certifier TRUSTe Goes For-Profit; Gets Investment From Accel ." 7/15/2008. Web. 7/1/2011. <http://paidcontent.org/article/419-privacy-certifier-truste-goes-for-profit-gets-investment-from-accel/>.

Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967. Print.

Williams, Felicia. *Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles*., 2006. Web. 2/08/2011.

Wingfield, Nick, and Julia Angwin. "Microsoft Adds Do-Not-Track Tool to Browser." *The Wall Street Journal,* 3/15/2011.Web. 5/4/2011.

<http://online.wsj.com/article/SB10001424052748703363904576200981919667762.html#ixzz1Gce29G4m>.

Zeigler, Andy, Adrian Bateman, and Eliot Graff. "Web Tracking Protection." 2/24/2011.Web. 3/3/2011. <http://www.w3.org/Submission/2011/SUBM-web-tracking-protection-20110224/>.

Zoosk.com. "About Zoosk." 2011. Web. 3/11/2011. <http://www.zoosk.com/about.php>.

Appendix I – Questionnaire

Comprehension Questions

1.) Collected information will be used to customize BrandX's service to me.

___ True ___ False

2.) Who is BrandX's parent company?

___ ParentX ___ BrandY ___ ParentCorp ___ ParentCompany ___ BrandX does not have a parent company

3.) Will BrandX share personal information when needed to comply with judicial or law enforcement requirements?

___ Yes ___ No

Trust of Summary Questions

Ability

1.) <Blank> is very capable of creating a summary of BrandX's privacy policy.

2.) <Blank> has much knowledge about creating summaries of privacy policies.

3.) I feel very confident about <Blank>'s skills in writing a summary for BrandX's privacy policy.

4.) <Blank> has specialized capabilities that can help it to write a summary for BrandX's privacy policy.

5.) <Blank> is well qualified to write a summary for BrandX's privacy policy.

Benevolence

1.) By summarizing BrandX’s privacy policy, I feel that <Blank> is very concerned about my welfare.

2.) Creating a summary of BrandX’s privacy policy shows that my needs and desires are very important to <Blank>.

3.) <Blank> would not knowingly do anything to hurt me while writing a summary of BrandX’s privacy policy.

4.) In summarizing BrandX’s privacy policy, <Blank> really looks out for what is important to me.

5.) <Blank> will go out of its way to help me understand my online privacy.

Integrity

1.) <Blank> applied a strong sense of justice while writing the summary of BrandX’s privacy policy.

2.) I do not have to wonder whether <Blank> will accurately summarize BrandX’s privacy policy.

3.) Sound principles seem to guide <Blank>’s writing of the summary of BrandX’s privacy policy.

Willingness to Pay Questions

1.) Assume that BrandX decides to offer its users access, for a fee, to a summary that <Blank> has written of its privacy policy. Would you be willing to pay some amount in the form of a fee added to BrandX’s monthly service fee in order to access a summary of BrandX’s privacy policy?

___ Yes ___ No

2.) <Presented if the answer to 1 is “No”> Did you answer no because you think you should not have to pay for access to summaries of privacy policies?

___ Yes ___ No

3.) <Presented if the answer to 1 is “Yes”> Please choose the value from the dropdown menu that is closest to the amount that you would pay, in the form of a fee added to BrandX’s monthly access charges, to have a summary of BrandX’s privacy policy provided to you while using BrandX’s site.

____ $0.05 ____ $0.10 ____ $0.20 ____ $0.30 ____ $0.40 ____ $0.50 ____ $0.60

____ $0.70 ____ $0.80 ____ $0.90 ____ $1.00 ____ More than $1.00

Privacy Concern Questions

1.) Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.

2.) When people give personal information to a company for some reason, the company should never use the information for any other reason.

3.) Companies should never sell the personal information in their computer databases to other companies.

4.) Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

Demographic Questions

1.) What is your age? ______

2.) Are you:

______ Female

______ Male

3.) Are you an undergraduate or graduate student?

4.) Please indicate the highest level of education completed by either of your parents.

______ Less than high school

______ Some high school

______ High school (includes GED)

______ Some college (includes Associate Degree)

______ College graduate (BS, BA, etc)

______ Some graduate education.

______ Graduate degree (MA, MS, PhD, JD, MD, etc.).

Appendix II - Summary of Match.com's Privacy Policy

Use of Collected Information

BrandX will use information it collects about visitors in several ways. BrandX will combine information it has collected with information from other sites owned by its parent company, ParentCorp, as well as business partners and other third parties. Collected and combined information will be used by BrandX to customize its services to visitors, target advertising on BrandX's site to visitors, and measure the effectiveness of BrandX's services and advertising.

Sharing of Collected Information

Non-personal information about visitors to BrandX's site, such as visitor trends and statistics, may be shared with third parties for advertising and business analysis. BrandX will also share personal information about visitors, but only for specific reasons. Personal information will be shared with business partners or third parties in order to provide BrandX's service and advertising, manage BrandX's business, and to complete any purchases you wish to make on BrandX's site. However, these third parties are not allowed to use personal information about our visitors in any other way. BrandX will also share personal information about its visitors with other sites owned by its parent company, ParentCorp. When required by law, BrandX will share personal information about visitors in order to comply with judicial or law enforcement actions. Finally, in the event of a corporate transaction, such as a merger, sale, or bankruptcy of BrandX, personal information about visitors maybe shared to complete the corporate transaction.

Appendix III - Differences Among the Four Questionnaires

Description about the Summary of Privacy Policy

This summary was written voluntarily by BrandX.

This summary was written by BrandX and is reviewed annually by a federal agency for accuracy.

This summary was written by a public university that is not affiliated with BrandX.

This summary was written by a public university that is not affiliated with BrandX and is reviewed annually by a federal agency for accuracy.

Description about the Trust of Summary Questions

Please indicate whether you agree or disagree with the following statements about the privacy policy summary that was voluntarily written by BrandX.

Please indicate whether you agree or disagree with the following statements about the privacy policy summary that was written by BrandX and is reviewed annually by a federal agency for accuracy.

Please indicate whether you agree or disagree with the following statements about the privacy policy summary that was written by an academic center as a public service.

Please indicate whether you agree or disagree with the following statements about the privacy policy summary that was written by an academic center as a public service and is reviewed annually by a federal agency for accuracy .

Trust of Summary Questions

Questions will refer to **“**BrandX” in the surveys asking about a first-party written survey.

Questions will refer to “the academic center” in the surveys asking about a third-party written survey.

Willingness To Pay Question

Assume that BrandX decides to offer its users access, for a fee, to a summary it has written of its privacy policy. Would you be willing to pay some amount in the form of a fee added to BrandX's monthly service fee in order to access a summary of BrandX's privacy policy?

Assume that BrandX decides to offer its users access, for a fee, to a summary it has written of its privacy policy that is reviewed annually by a federal agency for accuracy. Would you be willing to pay some amount in the form of a fee added to BrandX's monthly service fee in order to access a summary of BrandX's privacy policy?

Assume that BrandX decides to offer its users access, for a fee, to a summary that an academic center has written of its privacy policy. Would you be willing to pay some amount in the form of a fee added to BrandX's monthly service fee in order to access a summary of BrandX's privacy policy?

Assume that BrandX decides to offer its users access, for a fee, to a summary an academic center has written of its privacy policy that is reviewed annually by a federal agency for accuracy. Would you be willing to pay some amount in the form of a fee added to BrandX's monthly service fee in order to access a summary of BrandX's privacy policy?

Appendix IV - Cover Email

Hello, I am a master’s student here at the University of Minnesota, and I am really interested in helping students deal with the issue of online privacy. Because of that interest (and because I want to graduate), I am conducting an online survey of University of Minnesota students about their feelings on privacy, especially the trust they place in certain unknown organizations to help them understand the privacy policies of websites. I am sending you this email because I hope you will take 5 to 10 minutes to take the survey found at <URL>.

You will not be asked to share any personal information during the survey. This survey will only ask you about how much trust you place in an organization to help you with online privacy, how much you would be willing to pay that organization to help you, how concerned you are about privacy, and some basic demographic information. You are not required to take this survey for any reason, and you are not required to finish the survey once you start it.

That said, I hope you will take the short time to start and finish the survey. The data I hope to collect from students who take this survey will help me to develop better ways for policy makers, businesses, and computer professionals to address the growing issue of online privacy. At the end of the survey you will be presented with information and links to tools that help you to protect your privacy on the Internet. Also, if you submit a finished survey, you will be entered into a random drawing for a $25 gift card to Amazon.com, which will take place on May 31st.

To start the survey, please go to <URL>.

Thank You,

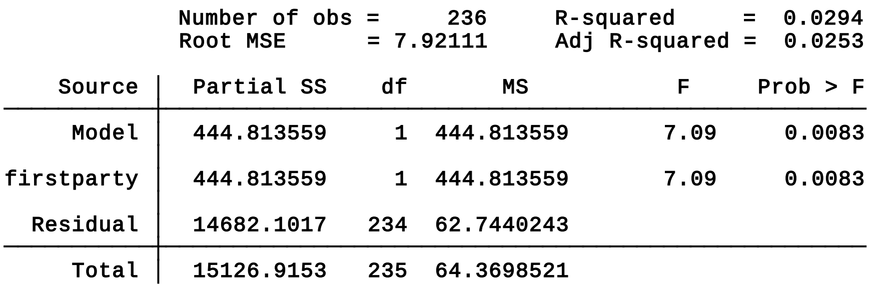
Bill Bushey

Appendix V - Variables

COMP_Q_Customize	Response to the first Comprehension question. The correct response is 1 (True).
COMP_Q_Parent	Response to the second Comprehension question. The correct response is 3 (ParentCorp).
COMP_Q_Share	Response to the third Comprehension question. The correct response is 1 (Yes).
COMP_Customize_Correct	Indicates whether the responded answered the first Comprehension question correctly.
COMP_Parent_Correct	Indicates whether the responded answered the second Comprehension question correctly.
COMP_Share_Correct	Indicates whether the responded answered the third Comprehension question correctly.
TRUST_ABILITY_Q_Capable	Response to Ability question number 1.
TRUST_ABILITY_Q_Knowledge	Response to Ability question number 2.
TRUST_ABILITY_Q_Confident	Response to Ability question number 3.
TRUST_ABILITY_Q_Specialized	Response to Ability question number 4.
TRUST_ABILITY_Q_Qualified	Response to Ability question number 5.
TRUST_BENEVOLENCE_Q_Concerned	Response to Benevolence question number 1.
TRUST_BENEVOLENCE_Q_Needs	Response to Benevolence question number 2.
TRUST_BENEVOLENCE_Q_Hurt	Response to Benevolence question number 3.
TRUST_BENEVOLENCE_Q_LooksOut	Response to Benevolence question number 4.
TRUST_BENEVOLENCE_Q_Help	Response to Benevolence question number 5.
TRUST_INTEGRITY_Q_Justice	Response to Integrity question number 1.
TRUST_INTEGRITY_Q_Accurately	Response to Integrity question number 2.
TRUST_INTEGRITY_Q_Principles	Response to Integrity question number 3.
TRUST_ABILITY_Sum	Summation of responses to all of the Ability questions.
TRUST_BENEVOLENCE_Sum	Summation of responses to all of the Benevolence questions.
TRUST_INTEGRITY_Sum	Summation of responses to all of the Integrity questions.
TRUST_Sum	Summation of responses to all of the Trust questions.
CV_WTP	Response to the Willingness to Pay question number 1, asking if the respondent will pay any amount for a privacy policy summary. 0 = No, 1 = Yes.
CV_Protest	Response to the Willingness to Pay question number 2, registering if the respondent is protesting the need to pay for a privacy policy summary.

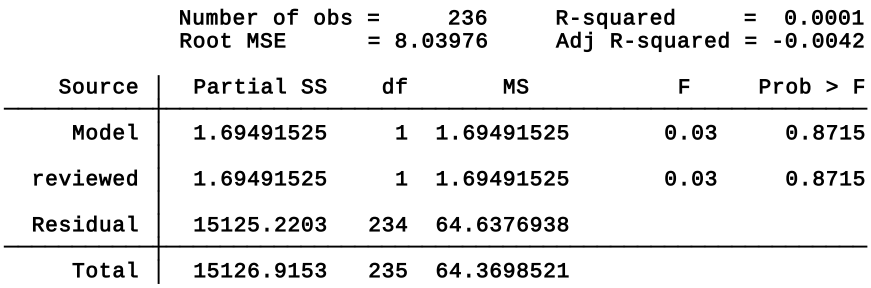
	0 = No Protest, 1 = Protest.
CV_Value	Response to the Willingness to Pay question number 3, the actual value a respondent would be willing to pay for a privacy policy summary.
CV_Value_f	Conversion of CV_Value from strings to floats. In the case of CV_WTP == 0, CV_Value_f = 0. In the case of CV_Value == “1+”, CV_Value_f = 1.5.
CONCERN_Q_AuthorizedUse	Response to Privacy Concern question number 1.
CONCERN_Q_Use	Response to Privacy Concern question number 2.
CONCERN_Q_Sell	Response to Privacy Concern question number 3.
CONCERN_Q_AuthorizedShare	Response to Privacy Concern question number 4.
CONCERN_Sum	Summation of responses to all of the Privacy Concern questions.
DEMO_Age	The respondent’s age in years.
DEMO_Gender	The respondent’s gender. 0 = Male, 1 = Female.
DEMO_Degree	Whether the respondent is an undergraduate or graduate student. 0 = Undergraduate, 1 = Graduate
DEMO_ParentEd	The highest level of attained by either of the respondent’s parents.
firstParty	Indicates if the response is from a first party treatment. 0 = Third Party, 1 = First Party
reviewed	Indicates if the response is from a reviewed treatment. 0 = Not Reviewed, 1 = Reviewed

Appendix VI - Stata Command Results



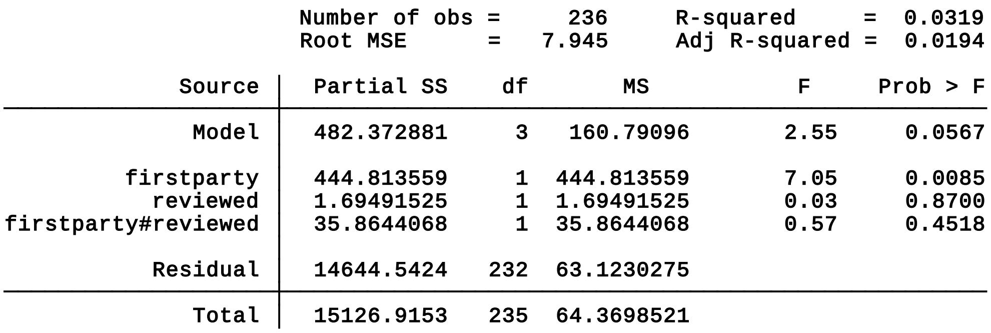
```
                         Number of obs =      236     R-squared     =  0.0294
                         Root MSE      = 7.92111     Adj R-squared =  0.0253

                Source | Partial SS    df       MS           F     Prob > F
            -----------+----------------------------------------------------
                 Model | 444.813559     1  444.813559       7.09     0.0083
                       |
            firstparty | 444.813559     1  444.813559       7.09     0.0083
                       |
              Residual | 14682.1017   234  62.7440243
            -----------+----------------------------------------------------
                 Total | 15126.9153   235  64.3698521
```

Figure A - Results for one-way ANOVA of TRUST_Sum on firstParty



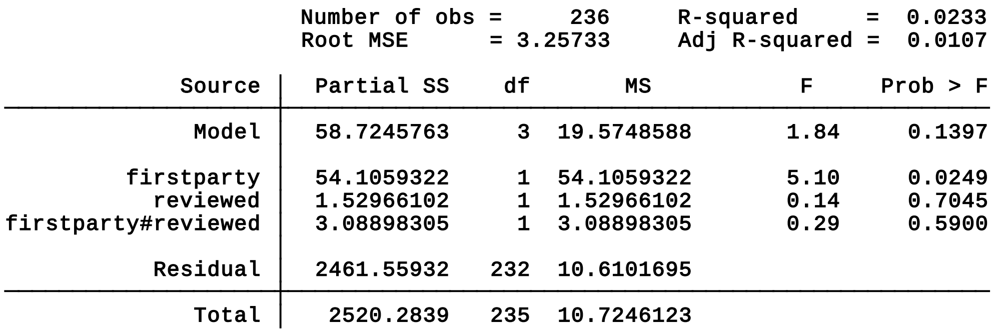
```
                         Number of obs =      236     R-squared     =  0.0001
                         Root MSE      = 8.03976     Adj R-squared = -0.0042

                Source | Partial SS    df       MS           F     Prob > F
            -----------+----------------------------------------------------
                 Model | 1.69491525     1  1.69491525       0.03     0.8715
                       |
              reviewed | 1.69491525     1  1.69491525       0.03     0.8715
                       |
              Residual | 15125.2203   234  64.6376938
            -----------+----------------------------------------------------
                 Total | 15126.9153   235  64.3698521
```

Figure B - Results for one-way ANOVA of TRUST_Sum on reviewed



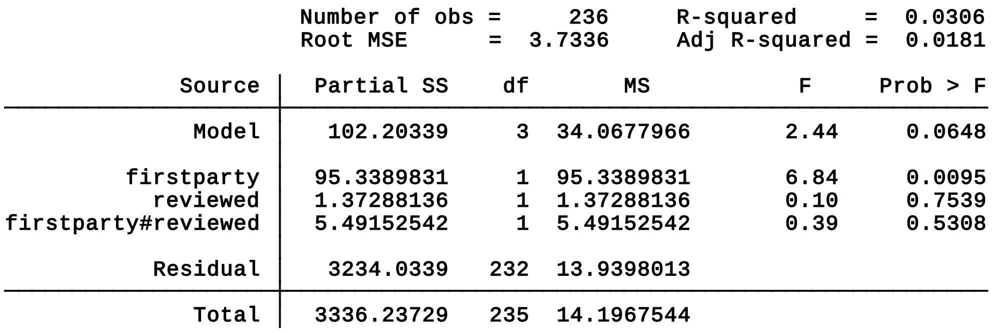
```
                         Number of obs =      236     R-squared     =  0.0319
                         Root MSE      =    7.945     Adj R-squared =  0.0194

                Source | Partial SS    df       MS           F     Prob > F
   --------------------+----------------------------------------------------
                 Model | 482.372881     3   160.79096       2.55     0.0567
                       |
            firstparty | 444.813559     1  444.813559       7.05     0.0085
              reviewed | 1.69491525     1  1.69491525       0.03     0.8700
   firstparty#reviewed | 35.8644068     1  35.8644068       0.57     0.4518
                       |
              Residual | 14644.5424   232  63.1230275
   --------------------+----------------------------------------------------
                 Total | 15126.9153   235  64.3698521
```

Figure C - Results for two-way ANOVA of TRUST_Sum on firstParty and reviewed, with interaction



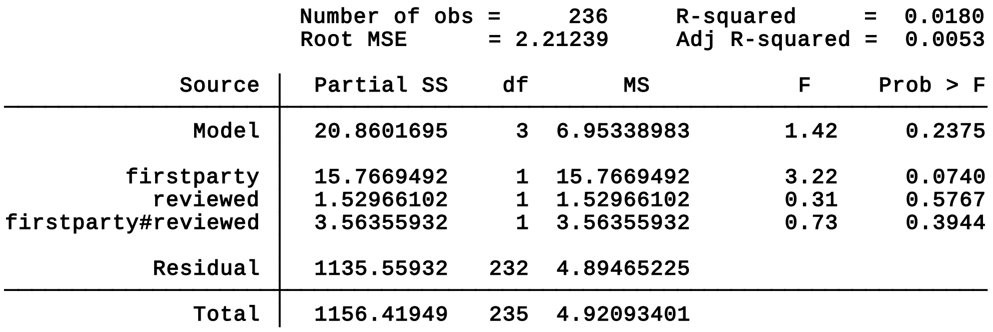
```
                           Number of obs =      236     R-squared     =  0.0233
                           Root MSE      = 3.25733     Adj R-squared =  0.0107

                  Source | Partial SS    df       MS           F     Prob > F
    ---------------------+----------------------------------------------------
                   Model | 58.7245763     3  19.5748588       1.84     0.1397
                         |
              firstparty | 54.1059322     1  54.1059322       5.10     0.0249
                reviewed | 1.52966102     1  1.52966102       0.14     0.7045
     firstparty#reviewed | 3.08898305     1  3.08898305       0.29     0.5900
                         |
                Residual | 2461.55932   232  10.6101695
    ---------------------+----------------------------------------------------
                   Total |  2520.2839   235  10.7246123
```

Figure D- Results for two-way ANOVA of TRUST_ABILITY_Sum on firstParty and reviewed, with interaction



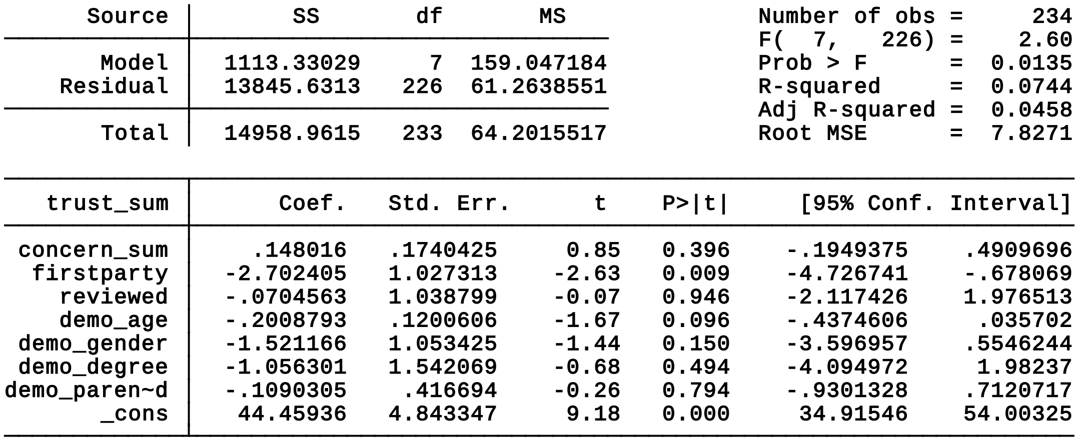
```
                           Number of obs =      236     R-squared     =  0.0306
                           Root MSE      =   3.7336    Adj R-squared =  0.0181

                  Source | Partial SS    df       MS           F     Prob > F
    ---------------------+----------------------------------------------------
                   Model |  102.20339     3  34.0677966       2.44     0.0648
                         |
              firstparty | 95.3389831     1  95.3389831       6.84     0.0095
                reviewed | 1.37288136     1  1.37288136       0.10     0.7539
     firstparty#reviewed | 5.49152542     1  5.49152542       0.39     0.5308
                         |
                Residual |  3234.0339   232  13.9398013
    ---------------------+----------------------------------------------------
                   Total | 3336.23729   235  14.1967544
```

Figure E - Results for two-way ANOVA of TRUST_BENEVOLENCE_Sum on firstParty and reviewed, with interaction



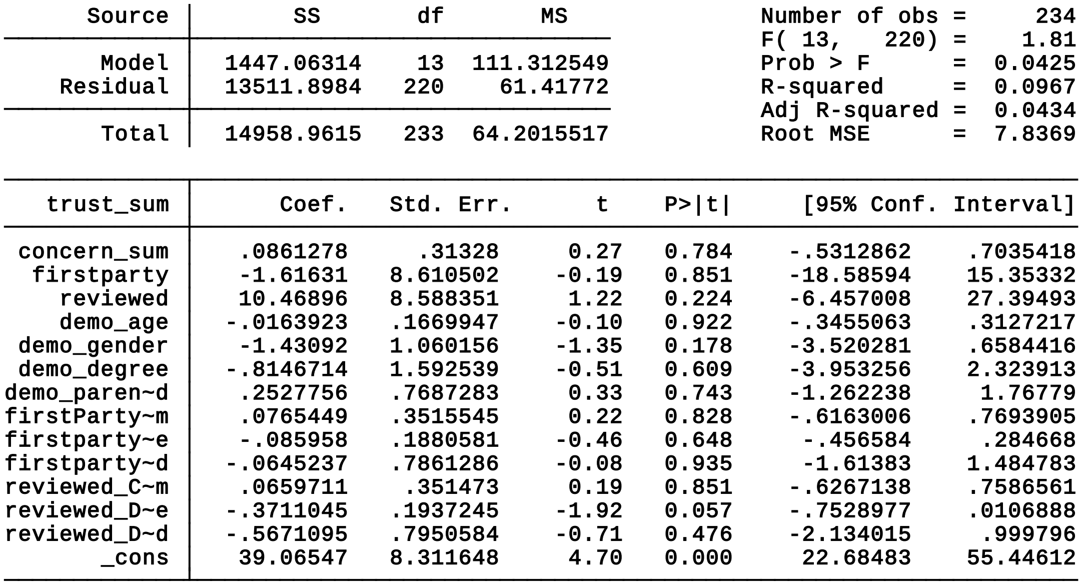
```
                           Number of obs =      236     R-squared     =  0.0180
                           Root MSE      = 2.21239     Adj R-squared =  0.0053

                  Source | Partial SS    df       MS           F     Prob > F
    ---------------------+----------------------------------------------------
                   Model | 20.8601695     3  6.95338983       1.42     0.2375
                         |
              firstparty | 15.7669492     1  15.7669492       3.22     0.0740
                reviewed | 1.52966102     1  1.52966102       0.31     0.5767
     firstparty#reviewed | 3.56355932     1  3.56355932       0.73     0.3944
                         |
                Residual | 1135.55932   232  4.89465225
    ---------------------+----------------------------------------------------
                   Total | 1156.41949   235  4.92093401
```

Figure F - Results for two-way ANOVA of TRUST_INTEGRITY_Sum on firstParty and reviewed, with interaction



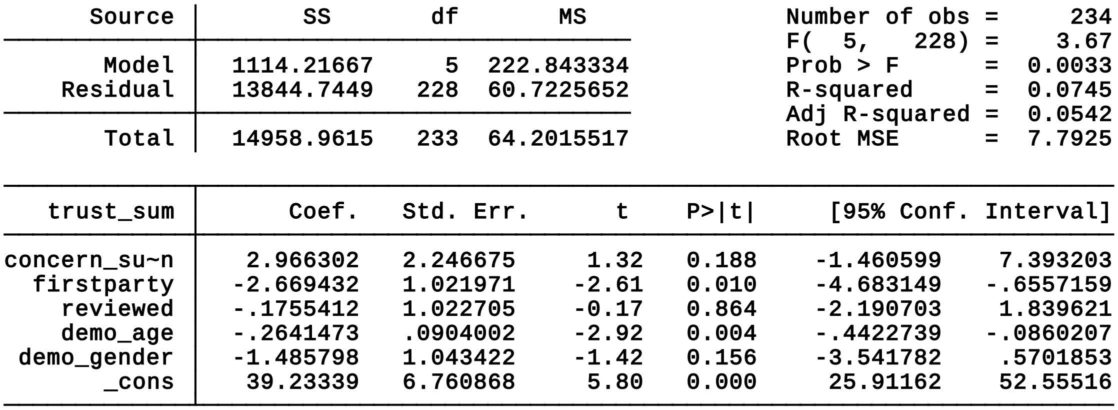
```
      Source |       SS       df       MS              Number of obs =     234
-------------+------------------------------           F(  7,   226) =    2.60
       Model |  1113.33029     7  159.047184           Prob > F      =  0.0135
    Residual |  13845.6313   226  61.2638551           R-squared     =  0.0744
-------------+------------------------------           Adj R-squared =  0.0458
       Total |  14958.9615   233  64.2015517           Root MSE      =  7.8271

------------------------------------------------------------------------------
   trust_sum |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
 concern_sum |    .148016   .1740425     0.85   0.396    -.1949375    .4909696
  firstparty |  -2.702405   1.027313    -2.63   0.009    -4.726741    -.678069
    reviewed |  -.0704563   1.038799    -0.07   0.946    -2.117426    1.976513
    demo_age |  -.2008793   .1200606    -1.67   0.096    -.4374606     .035702
 demo_gender |  -1.521166   1.053425    -1.44   0.150    -3.596957    .5546244
 demo_degree |  -1.056301   1.542069    -0.68   0.494    -4.094972     1.98237
demo_paren~d |  -.1090305    .416694    -0.26   0.794    -.9301328    .7120717
       _cons |   44.45936   4.843347     9.18   0.000     34.91546    54.00325
------------------------------------------------------------------------------
```

Figure G - Results for Regression on EQ1



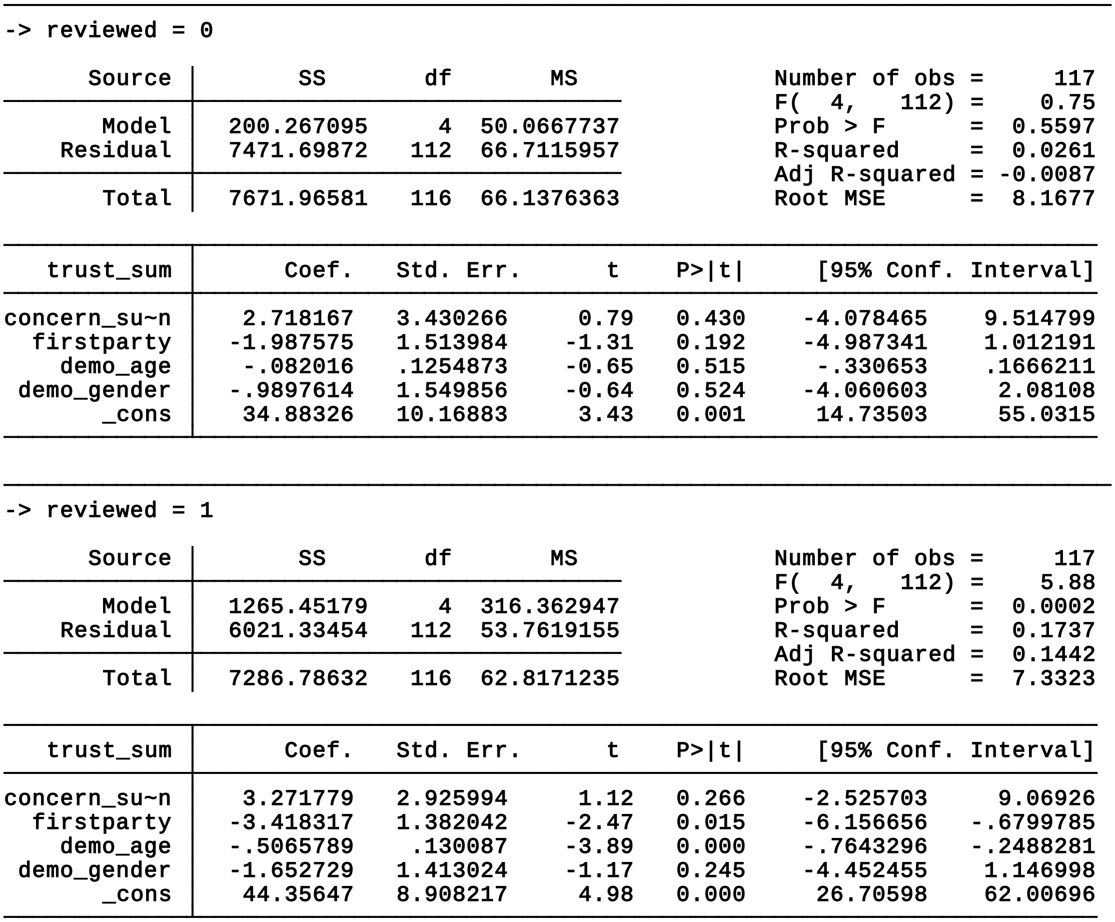
```
      Source |       SS       df       MS              Number of obs =     234
-------------+------------------------------           F( 13,   220) =    1.81
       Model |  1447.06314    13  111.312549           Prob > F      =  0.0425
    Residual |  13511.8984   220    61.41772           R-squared     =  0.0967
-------------+------------------------------           Adj R-squared =  0.0434
       Total |  14958.9615   233  64.2015517           Root MSE      =  7.8369

------------------------------------------------------------------------------
   trust_sum |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
 concern_sum |   .0861278     .31328     0.27   0.784    -.5312862    .7035418
  firstparty |   -1.61631   8.610502    -0.19   0.851    -18.58594    15.35332
    reviewed |   10.46896   8.588351     1.22   0.224    -6.457008    27.39493
    demo_age |  -.0163923   .1669947    -0.10   0.922    -.3455063    .3127217
 demo_gender |   -1.43092   1.060156    -1.35   0.178    -3.520281    .6584416
 demo_degree |  -.8146714   1.592539    -0.51   0.609    -3.953256    2.323913
demo_paren~d |   .2527756   .7687283     0.33   0.743    -1.262238     1.76779
firstParty~m |   .0765449   .3515545     0.22   0.828    -.6163006    .7693905
firstparty~e |   -.085958   .1880581    -0.46   0.648     -.456584     .284668
firstparty~d |  -.0645237   .7861286    -0.08   0.935     -1.61383    1.484783
reviewed_C~m |   .0659711    .351473     0.19   0.851    -.6267138    .7586561
reviewed_D~e |  -.3711045   .1937245    -1.92   0.057    -.7528977    .0106888
reviewed_D~d |  -.5671095   .7950584    -0.71   0.476    -2.134015     .999796
       _cons |   39.06547   8.311648     4.70   0.000     22.68483    55.44612
------------------------------------------------------------------------------
```

Figure H - Results for Regression on EQ1 with slope dummy variables added



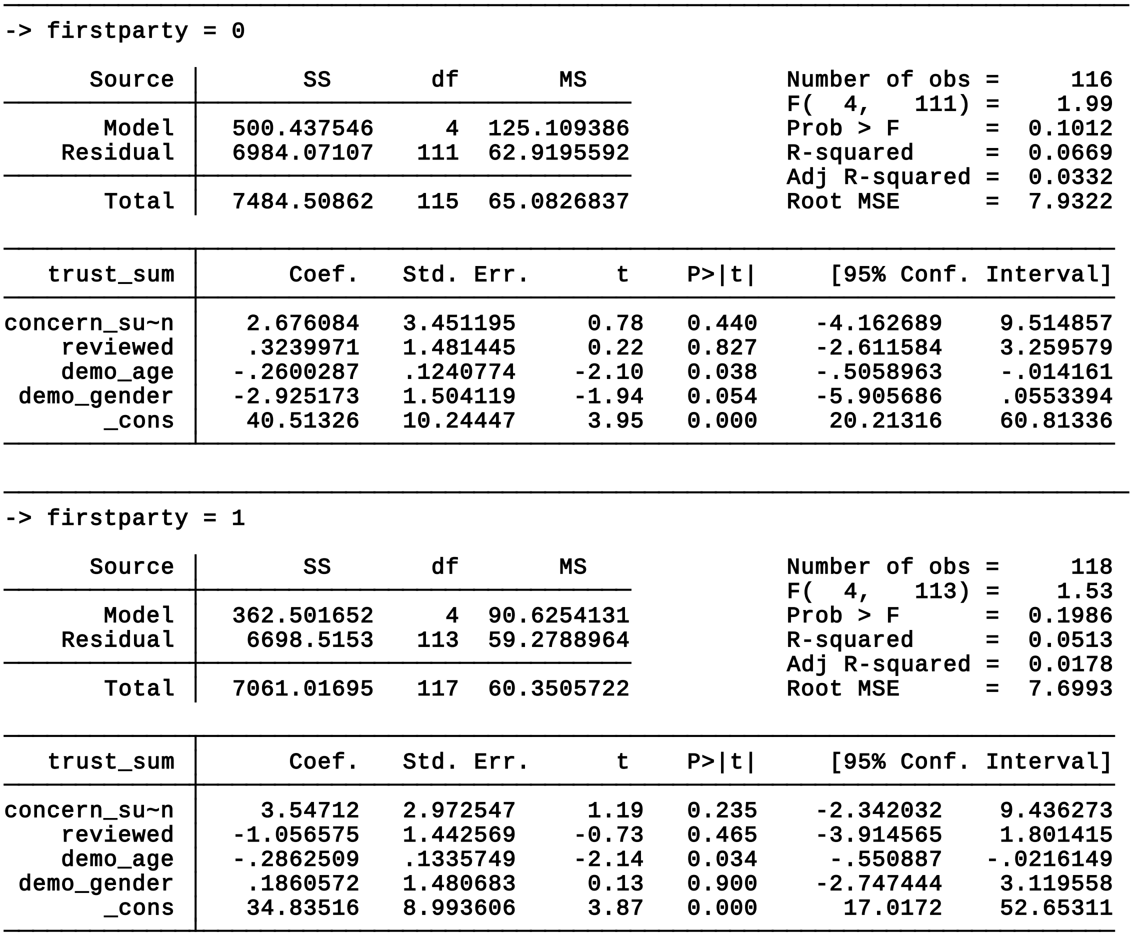
```
      Source |       SS       df       MS              Number of obs =     234
-------------+------------------------------           F(  5,   228) =    3.67
       Model |  1114.21667     5  222.843334           Prob > F      =  0.0033
    Residual |  13844.7449   228  60.7225652           R-squared     =  0.0745
-------------+------------------------------           Adj R-squared =  0.0542
       Total |  14958.9615   233  64.2015517           Root MSE      =  7.7925

------------------------------------------------------------------------------
   trust_sum |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   2.966302   2.246675     1.32   0.188    -1.460599    7.393203
  firstparty |  -2.669432   1.021971    -2.61   0.010    -4.683149   -.6557159
    reviewed |  -.1755412   1.022705    -0.17   0.864    -2.190703    1.839621
    demo_age |  -.2641473   .0904002    -2.92   0.004    -.4422739   -.0860207
 demo_gender |  -1.485798   1.043422    -1.42   0.156    -3.541782    .5701853
       _cons |   39.23339   6.760868     5.80   0.000     25.91162    52.55516
------------------------------------------------------------------------------
```

Figure I – Regression of the final TRUST_Sum equation



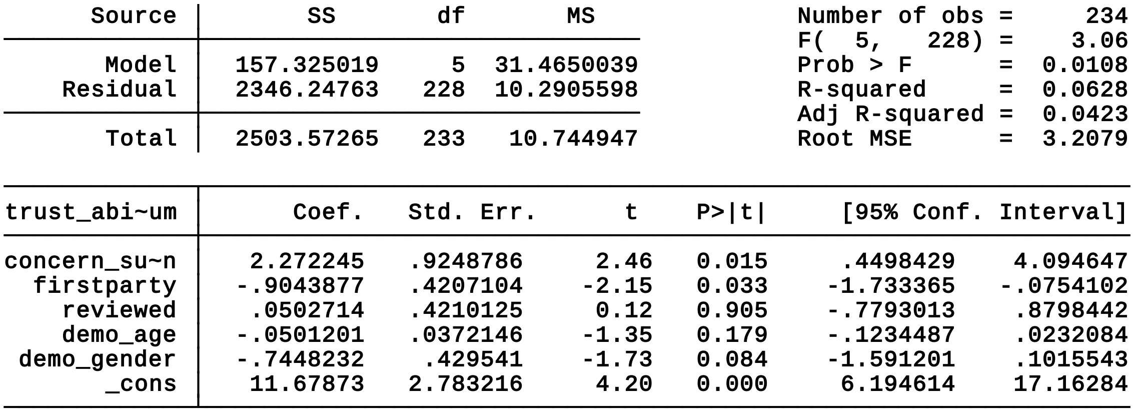
```
-------------------------------------------------------------------------------
-> reviewed = 0

      Source |       SS       df       MS              Number of obs =     117
-------------+------------------------------           F(  4,   112) =    0.75
       Model |  200.267095     4  50.0667737           Prob > F      =  0.5597
    Residual |  7471.69872   112  66.7115957           R-squared     =  0.0261
-------------+------------------------------           Adj R-squared = -0.0087
       Total |  7671.96581   116  66.1376363           Root MSE      =  8.1677

------------------------------------------------------------------------------
   trust_sum |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   2.718167   3.430266     0.79   0.430    -4.078465    9.514799
  firstparty |  -1.987575   1.513984    -1.31   0.192    -4.987341    1.012191
    demo_age |   -.082016   .1254873    -0.65   0.515     -.330653    .1666211
 demo_gender |  -.9897614   1.549856    -0.64   0.524    -4.060603     2.08108
       _cons |   34.88326   10.16883     3.43   0.001     14.73503     55.0315
------------------------------------------------------------------------------

-------------------------------------------------------------------------------
-> reviewed = 1

      Source |       SS       df       MS              Number of obs =     117
-------------+------------------------------           F(  4,   112) =    5.88
       Model |  1265.45179     4  316.362947           Prob > F      =  0.0002
    Residual |  6021.33454   112  53.7619155           R-squared     =  0.1737
-------------+------------------------------           Adj R-squared =  0.1442
       Total |  7286.78632   116  62.8171235           Root MSE      =  7.3323

------------------------------------------------------------------------------
   trust_sum |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   3.271779   2.925994     1.12   0.266    -2.525703     9.06926
  firstparty |  -3.418317   1.382042    -2.47   0.015    -6.156656   -.6799785
    demo_age |  -.5065789    .130087    -3.89   0.000    -.7643296   -.2488281
 demo_gender |  -1.652729   1.413024    -1.17   0.245    -4.452455    1.146998
       _cons |   44.35647   8.908217     4.98   0.000     26.70598    62.00696
------------------------------------------------------------------------------
```

Figure J - Results for Regression of Total Trust, reviewed Held Constant



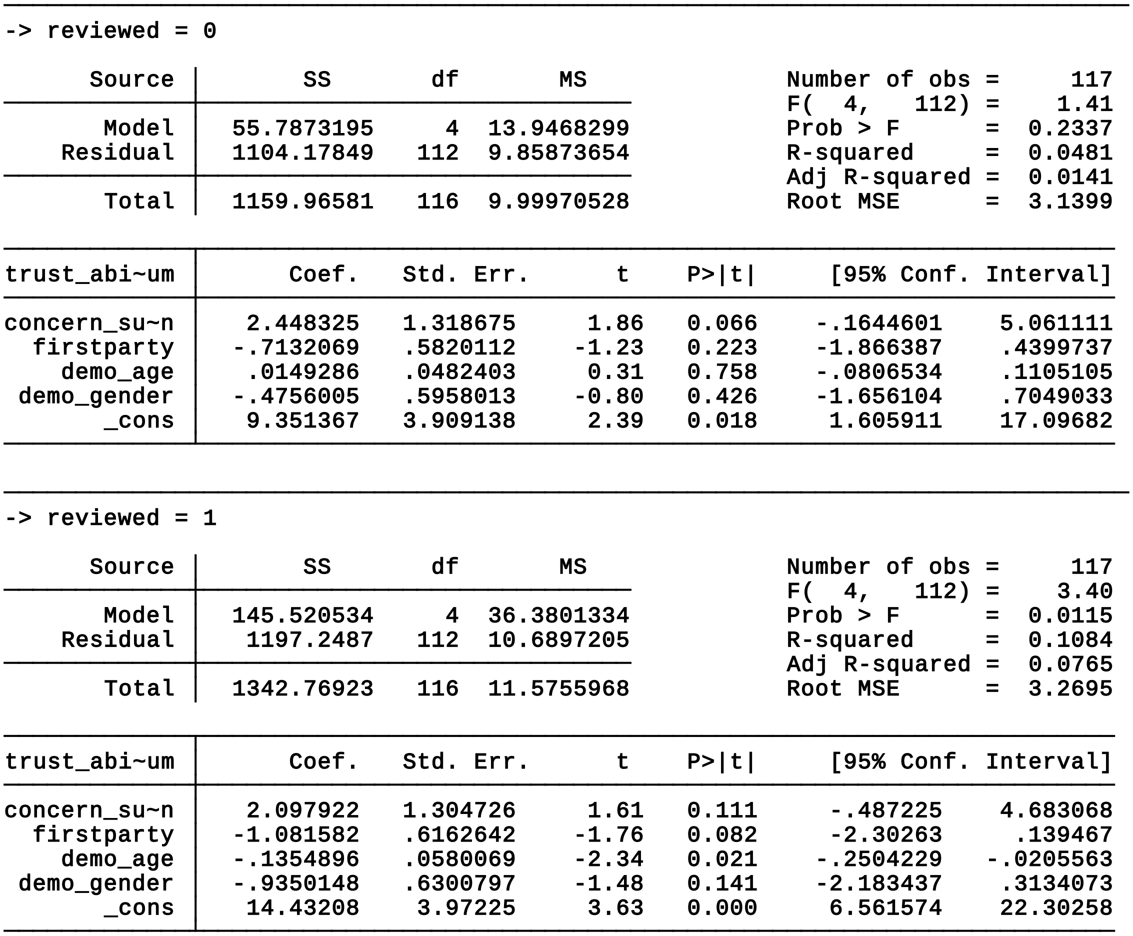
```
-> firstparty = 0

      Source |       SS       df       MS              Number of obs =     116
-------------+------------------------------           F(  4,   111) =    1.99
       Model |  500.437546     4  125.109386           Prob > F      =  0.1012
    Residual |  6984.07107   111  62.9195592           R-squared     =  0.0669
-------------+------------------------------           Adj R-squared =  0.0332
       Total |  7484.50862   115  65.0826837           Root MSE      =  7.9322

------------------------------------------------------------------------------
   trust_sum |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   2.676084   3.451195     0.78   0.440    -4.162689    9.514857
    reviewed |   .3239971   1.481445     0.22   0.827    -2.611584    3.259579
    demo_age |  -.2600287   .1240774    -2.10   0.038    -.5058963    -.014161
 demo_gender |  -2.925173   1.504119    -1.94   0.054    -5.905686    .0553394
       _cons |   40.51326   10.24447     3.95   0.000     20.21316    60.81336
------------------------------------------------------------------------------

-> firstparty = 1

      Source |       SS       df       MS              Number of obs =     118
-------------+------------------------------           F(  4,   113) =    1.53
       Model |  362.501652     4  90.6254131           Prob > F      =  0.1986
    Residual |   6698.5153   113  59.2788964           R-squared     =  0.0513
-------------+------------------------------           Adj R-squared =  0.0178
       Total |  7061.01695   117  60.3505722           Root MSE      =  7.6993

------------------------------------------------------------------------------
   trust_sum |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |    3.54712   2.972547     1.19   0.235    -2.342032    9.436273
    reviewed |  -1.056575   1.442569    -0.73   0.465    -3.914565    1.801415
    demo_age |  -.2862509   .1335749    -2.14   0.034     -.550887   -.0216149
 demo_gender |   .1860572   1.480683     0.13   0.900    -2.747444    3.119558
       _cons |   34.83516   8.993606     3.87   0.000      17.0172    52.65311
------------------------------------------------------------------------------
```

Figure K - Results for Regression of Total Trust, firstparty Held Constant



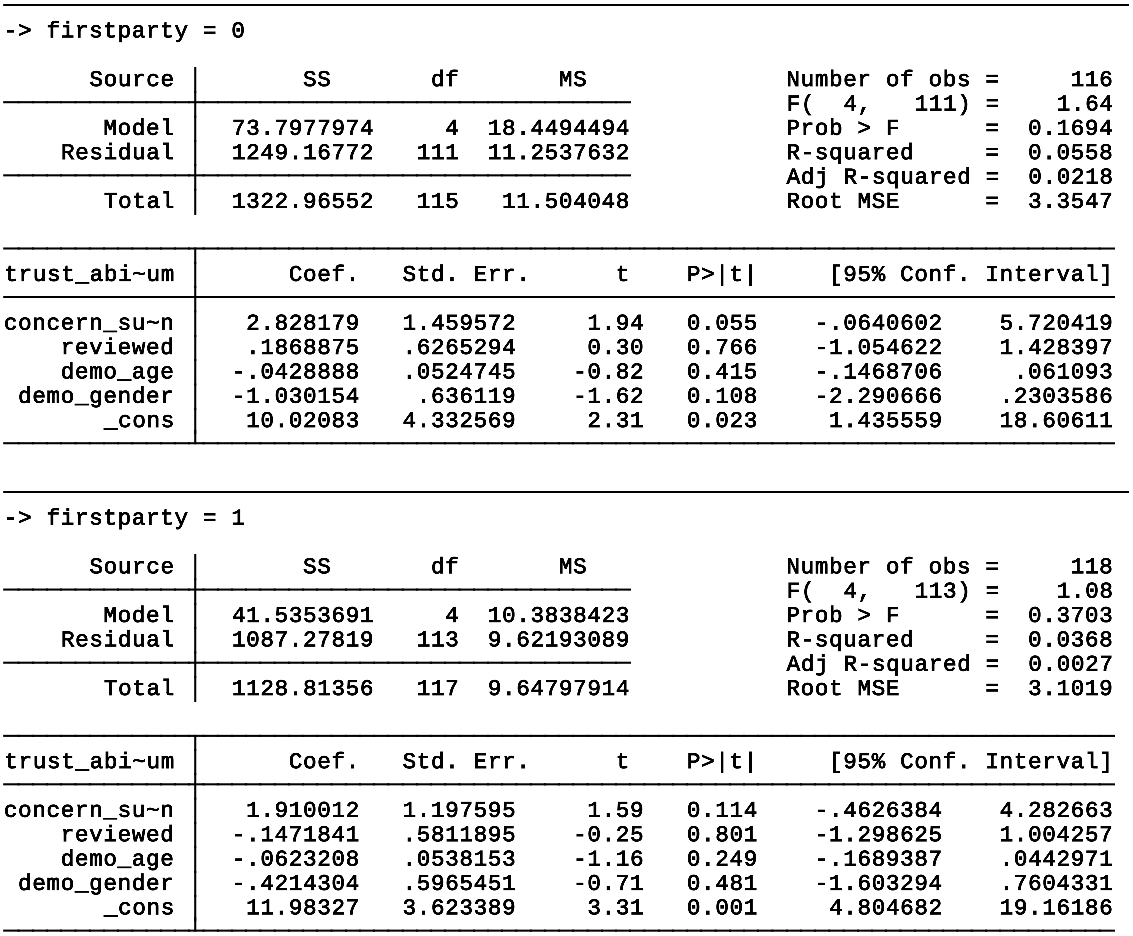
```
      Source |       SS       df       MS              Number of obs =     234
-------------+------------------------------           F(  5,   228) =    3.06
       Model |  157.325019     5  31.4650039           Prob > F      =  0.0108
    Residual |  2346.24763   228  10.2905598           R-squared     =  0.0628
-------------+------------------------------           Adj R-squared =  0.0423
       Total |  2503.57265   233   10.744947           Root MSE      =  3.2079

------------------------------------------------------------------------------
trust_abi~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   2.272245   .9248786     2.46   0.015     .4498429    4.094647
  firstparty |  -.9043877   .4207104    -2.15   0.033    -1.733365   -.0754102
    reviewed |   .0502714   .4210125     0.12   0.905    -.7793013    .8798442
    demo_age |  -.0501201   .0372146    -1.35   0.179    -.1234487    .0232084
 demo_gender |  -.7448232    .429541    -1.73   0.084    -1.591201    .1015543
       _cons |   11.67873   2.783216     4.20   0.000     6.194614    17.16284
------------------------------------------------------------------------------
```

Figure L - Results for Regression on Ability Trust



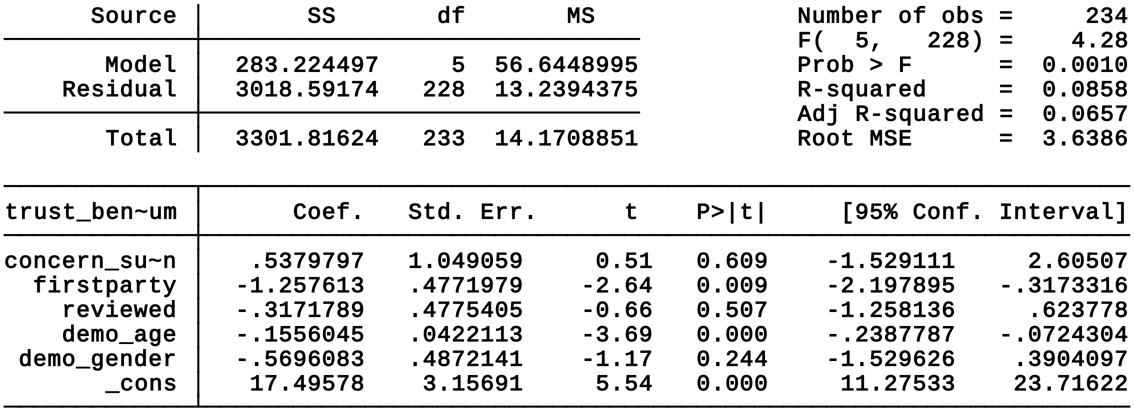
```
-> reviewed = 0

      Source |       SS           df       MS      Number of obs   =       117
-------------+----------------------------------   F(4, 112)       =      1.41
       Model |  55.7873195         4  13.9468299   Prob > F        =    0.2337
    Residual |  1104.17849       112  9.85873654   R-squared       =    0.0481
-------------+----------------------------------   Adj R-squared   =    0.0141
       Total |  1159.96581       116  9.99970528   Root MSE        =    3.1399

------------------------------------------------------------------------------
trust_abi~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   2.448325   1.318675     1.86   0.066    -.1644601    5.061111
  firstparty |  -.7132069   .5820112    -1.23   0.223    -1.866387    .4399737
    demo_age |   .0149286   .0482403     0.31   0.758    -.0806534    .1105105
 demo_gender |  -.4756005   .5958013    -0.80   0.426    -1.656104    .7049033
       _cons |   9.351367   3.909138     2.39   0.018     1.605911    17.09682
------------------------------------------------------------------------------

-> reviewed = 1

      Source |       SS           df       MS      Number of obs   =       117
-------------+----------------------------------   F(4, 112)       =      3.40
       Model |  145.520534         4  36.3801334   Prob > F        =    0.0115
    Residual |   1197.2487       112  10.6897205   R-squared       =    0.1084
-------------+----------------------------------   Adj R-squared   =    0.0765
       Total |  1342.76923       116  11.5755968   Root MSE        =    3.2695

------------------------------------------------------------------------------
trust_abi~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   2.097922   1.304726     1.61   0.111     -.487225    4.683068
  firstparty |  -1.081582   .6162642    -1.76   0.082     -2.30263     .139467
    demo_age |  -.1354896   .0580069    -2.34   0.021    -.2504229   -.0205563
 demo_gender |  -.9350148   .6300797    -1.48   0.141    -2.183437    .3134073
       _cons |   14.43208    3.97225     3.63   0.000     6.561574    22.30258
------------------------------------------------------------------------------
```

Figure M - Regression Results for Ability Trust, reviewed Held Constant



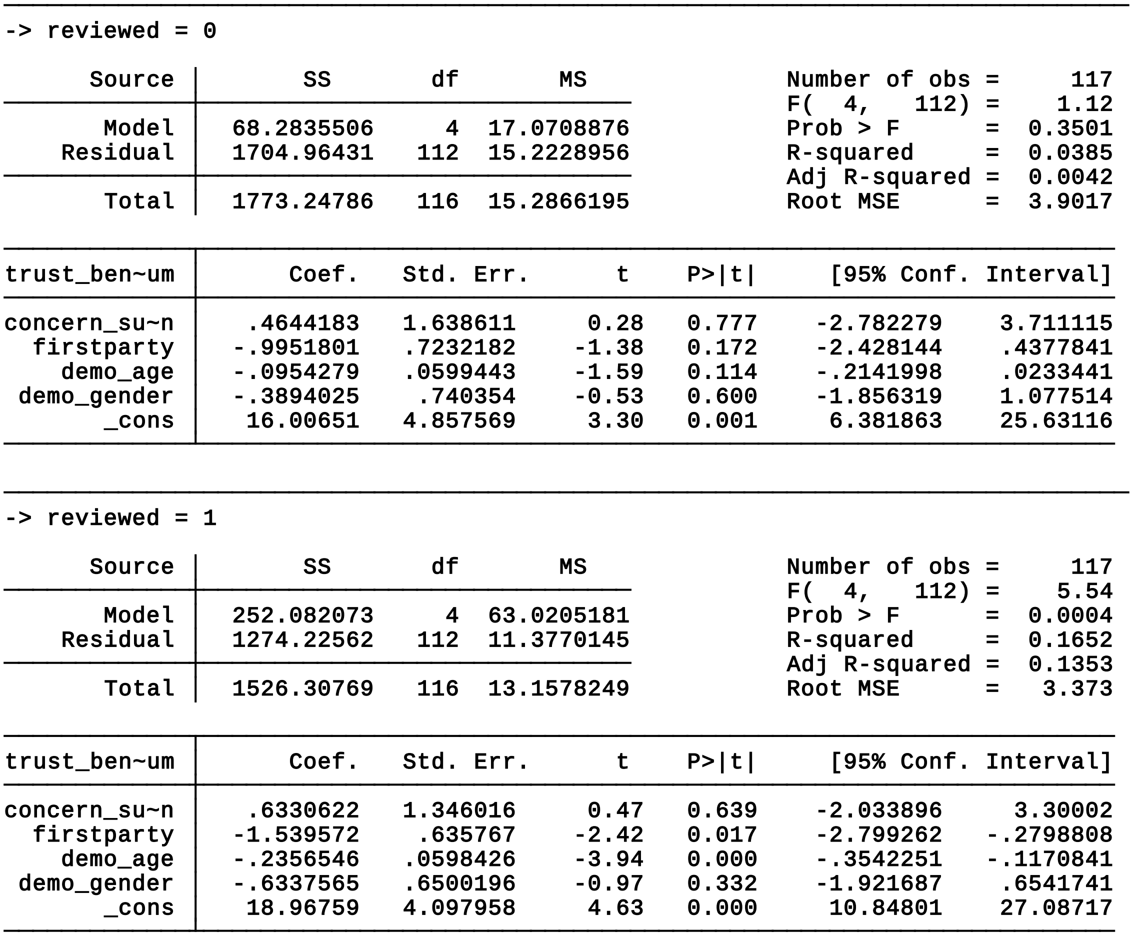
```
-> firstparty = 0

      Source |       SS       df       MS              Number of obs =     116
-------------+------------------------------           F(  4,   111) =    1.64
       Model |  73.7977974     4  18.4494494           Prob > F      =  0.1694
    Residual |  1249.16772   111  11.2537632           R-squared     =  0.0558
-------------+------------------------------           Adj R-squared =  0.0218
       Total |  1322.96552   115   11.504048           Root MSE      =  3.3547

------------------------------------------------------------------------------
trust_abi~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   2.828179   1.459572     1.94   0.055    -.0640602    5.720419
    reviewed |   .1868875   .6265294     0.30   0.766    -1.054622    1.428397
    demo_age |  -.0428888   .0524745    -0.82   0.415    -.1468706     .061093
 demo_gender |  -1.030154    .636119    -1.62   0.108    -2.290666    .2303586
       _cons |   10.02083   4.332569     2.31   0.023     1.435559    18.60611
------------------------------------------------------------------------------

-> firstparty = 1

      Source |       SS       df       MS              Number of obs =     118
-------------+------------------------------           F(  4,   113) =    1.08
       Model |  41.5353691     4  10.3838423           Prob > F      =  0.3703
    Residual |  1087.27819   113  9.62193089           R-squared     =  0.0368
-------------+------------------------------           Adj R-squared =  0.0027
       Total |  1128.81356   117  9.64797914           Root MSE      =  3.1019

------------------------------------------------------------------------------
trust_abi~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   1.910012   1.197595     1.59   0.114    -.4626384    4.282663
    reviewed |  -.1471841   .5811895    -0.25   0.801    -1.298625    1.004257
    demo_age |  -.0623208   .0538153    -1.16   0.249    -.1689387    .0442971
 demo_gender |  -.4214304   .5965451    -0.71   0.481    -1.603294    .7604331
       _cons |   11.98327   3.623389     3.31   0.001     4.804682    19.16186
------------------------------------------------------------------------------
```

Figure N - Regression Results for Ability Trust, firstParty Held Constant



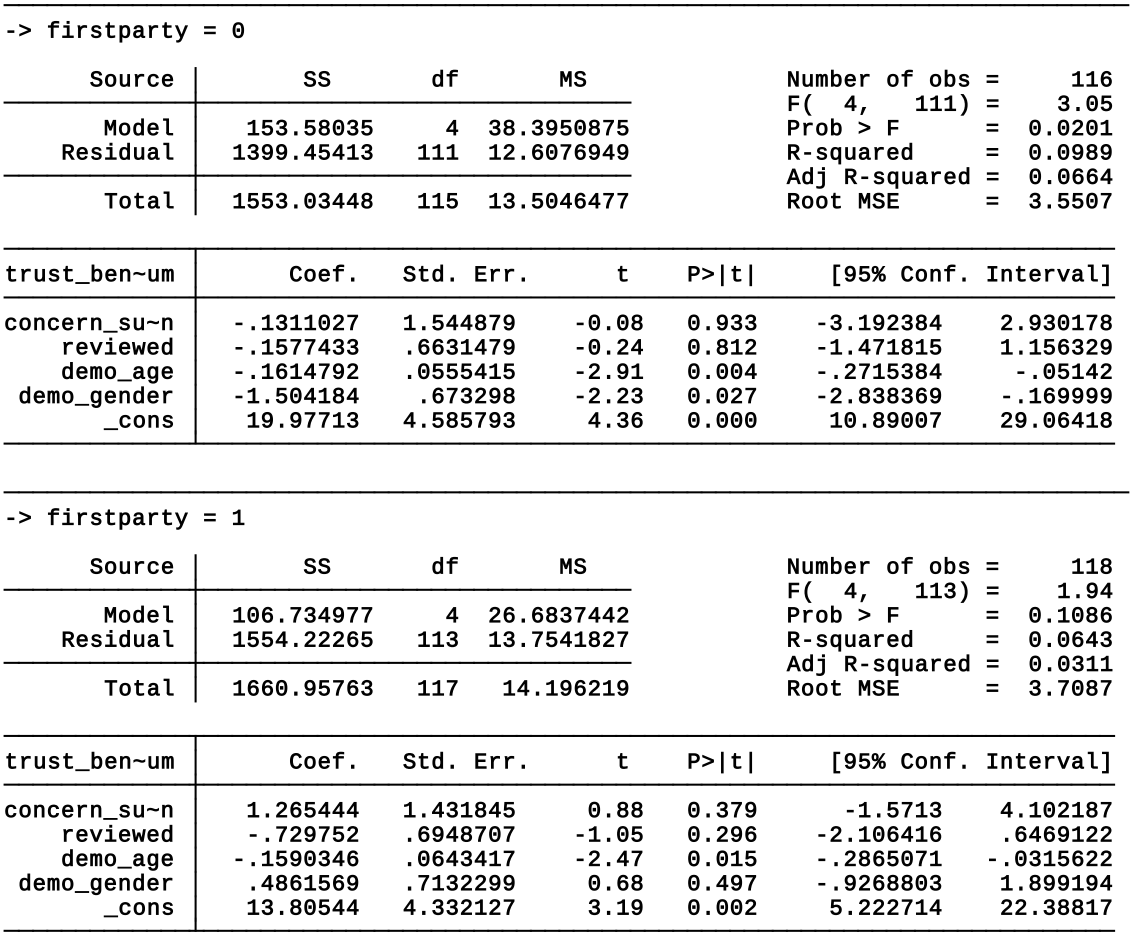
```
      Source |       SS       df       MS              Number of obs =     234
-------------+------------------------------           F(  5,   228) =    4.28
       Model |  283.224497     5  56.6448995           Prob > F      =  0.0010
    Residual |  3018.59174   228  13.2394375           R-squared     =  0.0858
-------------+------------------------------           Adj R-squared =  0.0657
       Total |  3301.81624   233  14.1708851           Root MSE      =  3.6386

------------------------------------------------------------------------------
trust_ben~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   .5379797   1.049059     0.51   0.609    -1.529111     2.60507
  firstparty |  -1.257613   .4771979    -2.64   0.009    -2.197895   -.3173316
    reviewed |  -.3171789   .4775405    -0.66   0.507    -1.258136     .623778
    demo_age |  -.1556045   .0422113    -3.69   0.000    -.2387787   -.0724304
 demo_gender |  -.5696083   .4872141    -1.17   0.244    -1.529626    .3904097
       _cons |   17.49578    3.15691     5.54   0.000     11.27533    23.71622
------------------------------------------------------------------------------
```

Figure O - Regression Results for Benevolence Trust



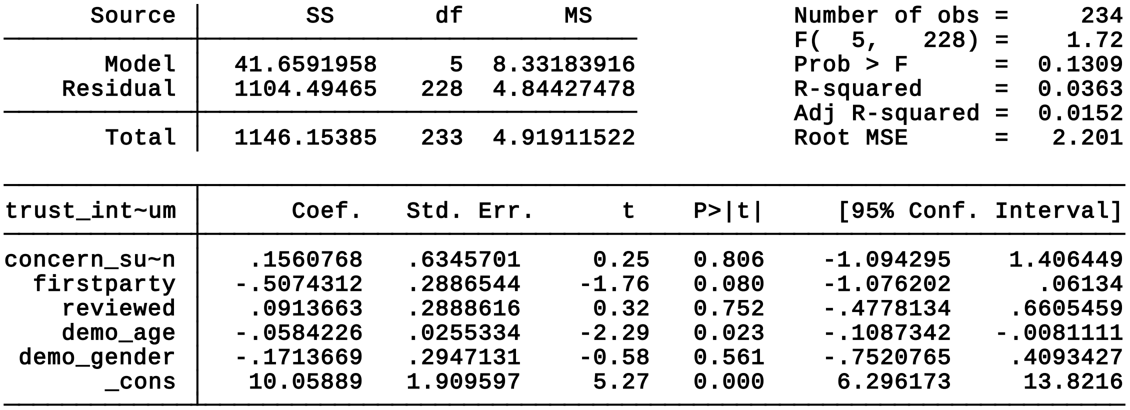
```
-> reviewed = 0

      Source |       SS       df       MS              Number of obs =     117
-------------+------------------------------           F(  4,   112) =    1.12
       Model |  68.2835506     4  17.0708876           Prob > F      =  0.3501
    Residual |  1704.96431   112  15.2228956           R-squared     =  0.0385
-------------+------------------------------           Adj R-squared =  0.0042
       Total |  1773.24786   116  15.2866195           Root MSE      =  3.9017

------------------------------------------------------------------------------
trust_ben~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   .4644183   1.638611     0.28   0.777    -2.782279    3.711115
  firstparty |  -.9951801   .7232182    -1.38   0.172    -2.428144    .4377841
    demo_age |  -.0954279   .0599443    -1.59   0.114    -.2141998    .0233441
 demo_gender |  -.3894025    .740354    -0.53   0.600    -1.856319    1.077514
       _cons |   16.00651   4.857569     3.30   0.001     6.381863    25.63116
------------------------------------------------------------------------------

-------------------------------------------------------------------------------
-> reviewed = 1

      Source |       SS       df       MS              Number of obs =     117
-------------+------------------------------           F(  4,   112) =    5.54
       Model |  252.082073     4  63.0205181           Prob > F      =  0.0004
    Residual |  1274.22562   112  11.3770145           R-squared     =  0.1652
-------------+------------------------------           Adj R-squared =  0.1353
       Total |  1526.30769   116  13.1578249           Root MSE      =   3.373

------------------------------------------------------------------------------
trust_ben~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   .6330622   1.346016     0.47   0.639    -2.033896     3.30002
  firstparty |  -1.539572    .635767    -2.42   0.017    -2.799262   -.2798808
    demo_age |  -.2356546   .0598426    -3.94   0.000    -.3542251   -.1170841
 demo_gender |  -.6337565   .6500196    -0.97   0.332    -1.921687    .6541741
       _cons |   18.96759   4.097958     4.63   0.000     10.84801    27.08717
------------------------------------------------------------------------------
```

Figure P - Regression Results for Benevolence Trust, with reviewed Held Constant



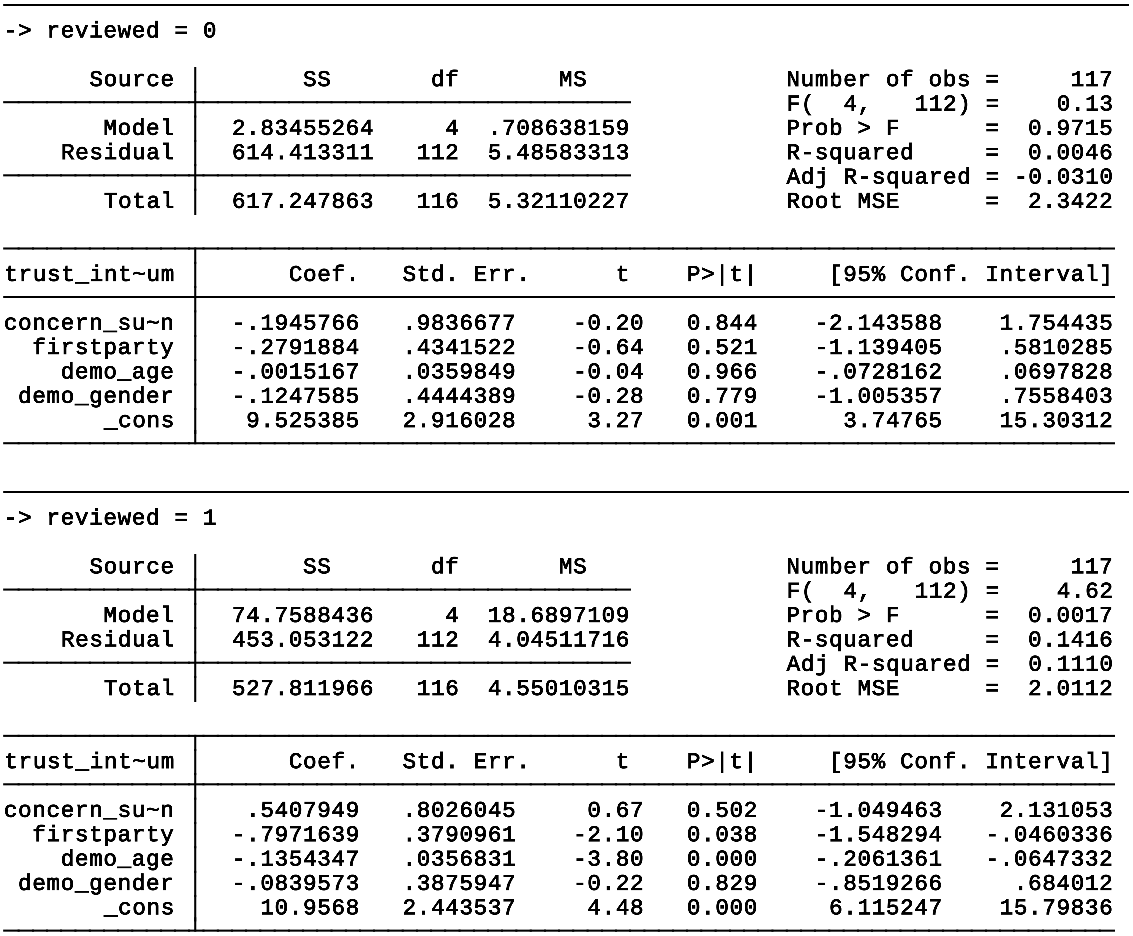
```
--------------------------------------------------------------------------------
-> firstparty = 0

      Source |       SS           df       MS      Number of obs   =       116
-------------+----------------------------------   F(4, 111)       =      3.05
       Model |   153.58035         4  38.3950875   Prob > F        =    0.0201
    Residual |  1399.45413       111  12.6076949   R-squared       =    0.0989
-------------+----------------------------------   Adj R-squared   =    0.0664
       Total |  1553.03448       115  13.5046477   Root MSE        =    3.5507

------------------------------------------------------------------------------
trust_ben~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |  -.1311027   1.544879    -0.08   0.933    -3.192384    2.930178
    reviewed |  -.1577433   .6631479    -0.24   0.812    -1.471815    1.156329
    demo_age |  -.1614792   .0555415    -2.91   0.004    -.2715384    -.05142
 demo_gender |  -1.504184    .673298    -2.23   0.027    -2.838369   -.169999
       _cons |   19.97713   4.585793     4.36   0.000     10.89007    29.06418
------------------------------------------------------------------------------

--------------------------------------------------------------------------------
-> firstparty = 1

      Source |       SS           df       MS      Number of obs   =       118
-------------+----------------------------------   F(4, 113)       =      1.94
       Model |  106.734977         4  26.6837442   Prob > F        =    0.1086
    Residual |  1554.22265       113  13.7541827   R-squared       =    0.0643
-------------+----------------------------------   Adj R-squared   =    0.0311
       Total |  1660.95763       117   14.196219   Root MSE        =    3.7087

------------------------------------------------------------------------------
trust_ben~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   1.265444   1.431845     0.88   0.379      -1.5713    4.102187
    reviewed |   -.729752   .6948707    -1.05   0.296    -2.106416    .6469122
    demo_age |  -.1590346   .0643417    -2.47   0.015    -.2865071   -.0315622
 demo_gender |   .4861569   .7132299     0.68   0.497    -.9268803    1.899194
       _cons |   13.80544   4.332127     3.19   0.002     5.222714    22.38817
------------------------------------------------------------------------------
```

Figure Q - Regression Results for Benevolence Trust, firstParty Held Constant



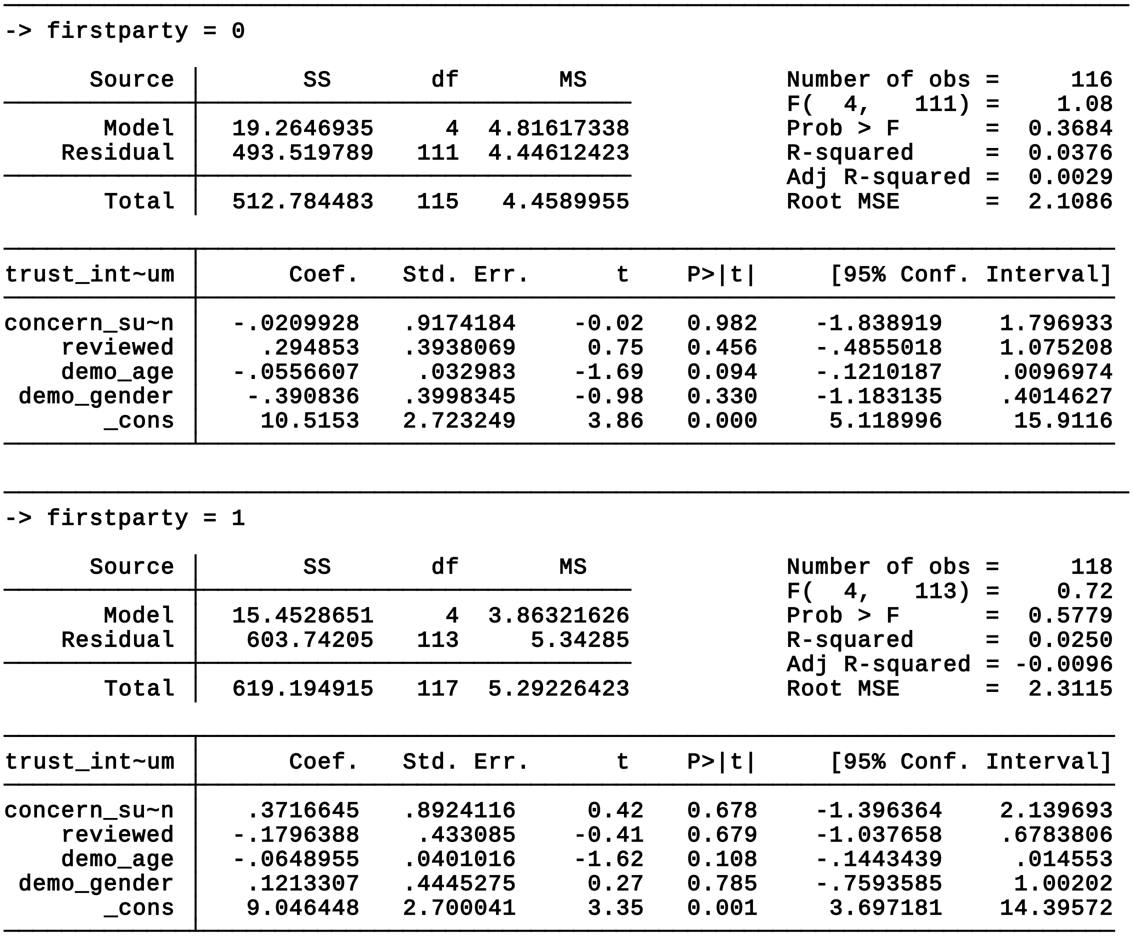
```
      Source |       SS           df       MS      Number of obs   =       234
-------------+----------------------------------   F(5, 228)       =      1.72
       Model |  41.6591958         5  8.33183916   Prob > F        =    0.1309
    Residual |  1104.49465       228  4.84427478   R-squared       =    0.0363
-------------+----------------------------------   Adj R-squared   =    0.0152
       Total |  1146.15385       233  4.91911522   Root MSE        =     2.201

------------------------------------------------------------------------------
trust_int~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   .1560768   .6345701     0.25   0.806    -1.094295    1.406449
  firstparty |  -.5074312   .2886544    -1.76   0.080    -1.076202      .06134
    reviewed |   .0913663   .2888616     0.32   0.752    -.4778134    .6605459
    demo_age |  -.0584226   .0255334    -2.29   0.023    -.1087342   -.0081111
 demo_gender |  -.1713669   .2947131    -0.58   0.561    -.7520765    .4093427
       _cons |   10.05889   1.909597     5.27   0.000     6.296173     13.8216
------------------------------------------------------------------------------
```

Figure R - Regression Results for Integrity Trust



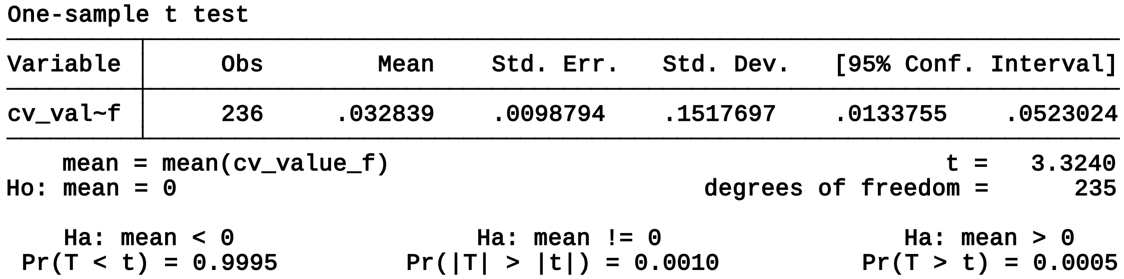
```
-> reviewed = 0

      Source |       SS           df       MS      Number of obs   =       117
-------------+----------------------------------   F(4, 112)       =      0.13
       Model |  2.83455264         4  .708638159   Prob > F        =    0.9715
    Residual |  614.413311       112  5.48583313   R-squared       =    0.0046
-------------+----------------------------------   Adj R-squared   =   -0.0310
       Total |  617.247863       116  5.32110227   Root MSE        =    2.3422

------------------------------------------------------------------------------
trust_int~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |  -.1945766   .9836677    -0.20   0.844    -2.143588    1.754435
  firstparty |  -.2791884   .4341522    -0.64   0.521    -1.139405    .5810285
    demo_age |  -.0015167   .0359849    -0.04   0.966    -.0728162    .0697828
 demo_gender |  -.1247585   .4444389    -0.28   0.779    -1.005357    .7558403
       _cons |   9.525385   2.916028     3.27   0.001      3.74765    15.30312
------------------------------------------------------------------------------

-> reviewed = 1

      Source |       SS           df       MS      Number of obs   =       117
-------------+----------------------------------   F(4, 112)       =      4.62
       Model |  74.7588436         4  18.6897109   Prob > F        =    0.0017
    Residual |  453.053122       112  4.04511716   R-squared       =    0.1416
-------------+----------------------------------   Adj R-squared   =    0.1110
       Total |  527.811966       116  4.55010315   Root MSE        =    2.0112

------------------------------------------------------------------------------
trust_int~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   .5407949   .8026045     0.67   0.502    -1.049463    2.131053
  firstparty |  -.7971639   .3790961    -2.10   0.038    -1.548294   -.0460336
    demo_age |  -.1354347   .0356831    -3.80   0.000    -.2061361   -.0647332
 demo_gender |  -.0839573   .3875947    -0.22   0.829    -.8519266     .684012
       _cons |    10.9568   2.443537     4.48   0.000     6.115247    15.79836
------------------------------------------------------------------------------
```

Figure S - Regression Results for Integrity Trust, with reviewed Held Constant



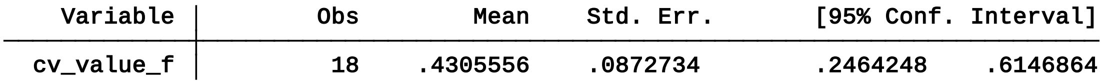
```
-> firstparty = 0

      Source |       SS       df       MS              Number of obs =     116
-------------+------------------------------           F(  4,   111) =    1.08
       Model |  19.2646935     4  4.81617338           Prob > F      =  0.3684
    Residual |  493.519789   111  4.44612423           R-squared     =  0.0376
-------------+------------------------------           Adj R-squared =  0.0029
       Total |  512.784483   115   4.4589955           Root MSE      =  2.1086

------------------------------------------------------------------------------
trust_int~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |  -.0209928   .9174184    -0.02   0.982    -1.838919    1.796933
    reviewed |    .294853   .3938069     0.75   0.456    -.4855018    1.075208
    demo_age |  -.0556607    .032983    -1.69   0.094    -.1210187    .0096974
 demo_gender |   -.390836   .3998345    -0.98   0.330    -1.183135    .4014627
       _cons |    10.5153   2.723249     3.86   0.000     5.118996     15.9116
------------------------------------------------------------------------------

-> firstparty = 1

      Source |       SS       df       MS              Number of obs =     118
-------------+------------------------------           F(  4,   113) =    0.72
       Model |  15.4528651     4  3.86321626           Prob > F      =  0.5779
    Residual |   603.74205   113     5.34285           R-squared     =  0.0250
-------------+------------------------------           Adj R-squared = -0.0096
       Total |  619.194915   117  5.29226423           Root MSE      =  2.3115

------------------------------------------------------------------------------
trust_int~um |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |   .3716645   .8924116     0.42   0.678    -1.396364    2.139693
    reviewed |  -.1796388    .433085    -0.41   0.679    -1.037658    .6783806
    demo_age |  -.0648955   .0401016    -1.62   0.108    -.1443439     .014553
 demo_gender |   .1213307   .4445275     0.27   0.785    -.7593585     1.00202
       _cons |   9.046448   2.700041     3.35   0.001     3.697181    14.39572
------------------------------------------------------------------------------
```

Figure T - Regression Results for Integrity Trust, firstParty Held Constant



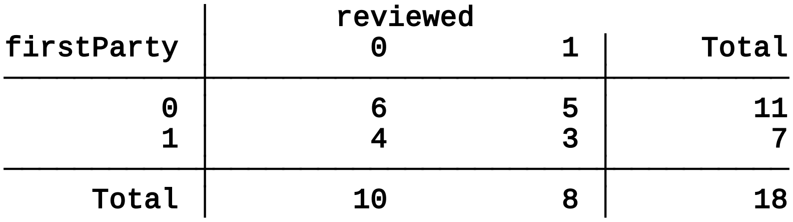
```
One-sample t test
------------------------------------------------------------------------------
Variable |     Obs        Mean    Std. Err.   Std. Dev.   [95% Conf. Interval]
---------+--------------------------------------------------------------------
cv_val~f |     236     .032839    .0098794    .1517697    .0133755    .0523024
------------------------------------------------------------------------------
    mean = mean(cv_value_f)                                       t =   3.3240
Ho: mean = 0                                     degrees of freedom =      235

    Ha: mean < 0                 Ha: mean != 0                 Ha: mean > 0
 Pr(T < t) = 0.9995         Pr(|T| > |t|) = 0.0010          Pr(T > t) = 0.0005
```

Figure U - Results of a ttest on the value of CV_Value_f == 0



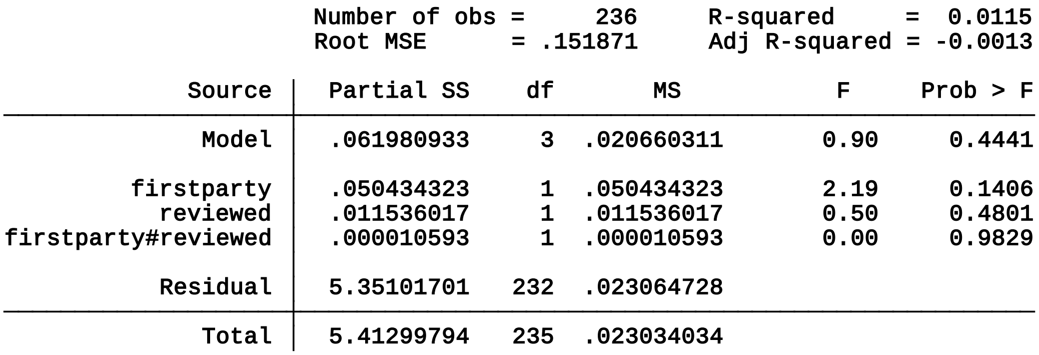
```
    Variable |        Obs        Mean    Std. Err.       [95% Conf. Interval]
-------------+---------------------------------------------------------------
  cv_value_f |         18    .4305556    .0872734        .2464248    .6146864
```

Figure V- Mean and 95% Confidence Interval for CV_Value among respondents who were willing to pay



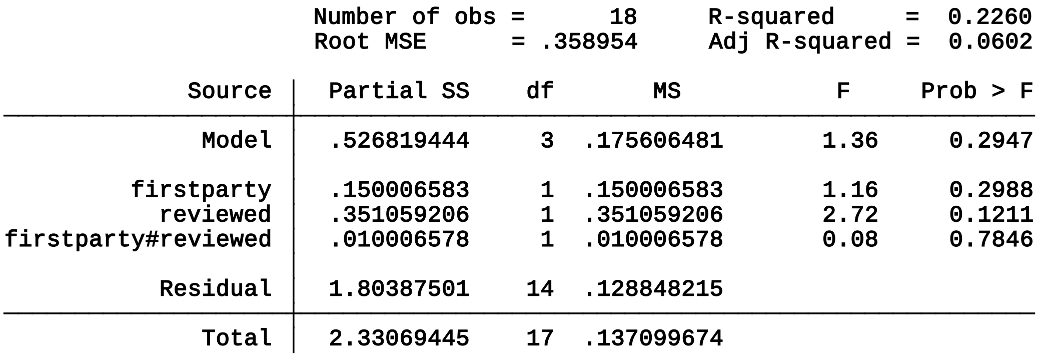
```
           |       reviewed
firstParty |         0          1 |     Total
-----------+----------------------+----------
         0 |         6          5 |        11 
         1 |         4          3 |         7 
-----------+----------------------+----------
     Total |        10          8 |        18 
```

Figure W - Occurrence of willing to pay respondents among the treatment subsamples



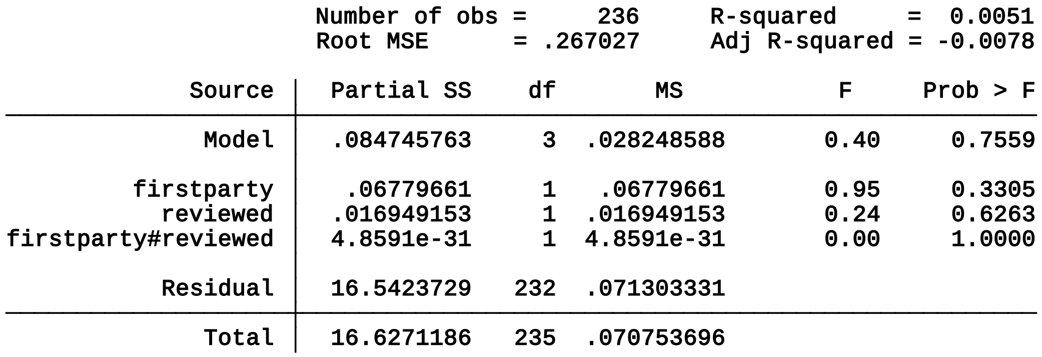
```
                         Number of obs =        236    R-squared     =  0.0115
                         Root MSE      =    .151871    Adj R-squared = -0.0013

                  Source |  Partial SS    df       MS           F     Prob > F
     --------------------+----------------------------------------------------
                   Model |   .061980933     3   .020660311      0.90    0.4441
                         |
              firstparty |   .050434323     1   .050434323      2.19    0.1406
                reviewed |   .011536017     1   .011536017      0.50    0.4801
     firstparty#reviewed |   .000010593     1   .000010593      0.00    0.9829
                         |
                Residual |   5.35101701   232   .023064728   
     --------------------+----------------------------------------------------
                   Total |   5.41299794   235   .023034034   
```

Figure X - Results from two-way ANOVA of CV_Value_f on firstParty and reviewed, all respondents



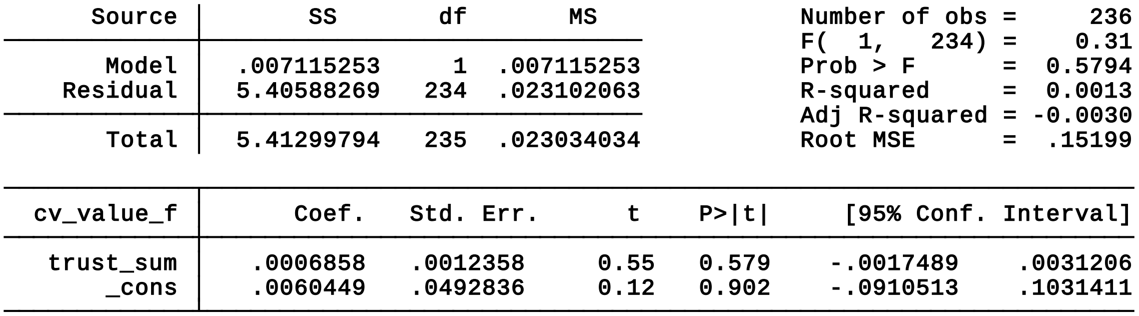
```
                         Number of obs =         18    R-squared     =  0.2260
                         Root MSE      =    .358954    Adj R-squared =  0.0602

                  Source |  Partial SS    df       MS           F     Prob > F
     --------------------+----------------------------------------------------
                   Model |   .526819444     3   .175606481      1.36    0.2947
                         |
              firstparty |   .150006583     1   .150006583      1.16    0.2988
                reviewed |   .351059206     1   .351059206      2.72    0.1211
     firstparty#reviewed |   .010006578     1   .010006578      0.08    0.7846
                         |
                Residual |   1.80387501    14   .128848215   
     --------------------+----------------------------------------------------
                   Total |   2.33069445    17   .137099674   
```

Figure Y - Results from two-way ANOVA of CV_Value_f on firstParty and reviewed, only willing to pay respondents



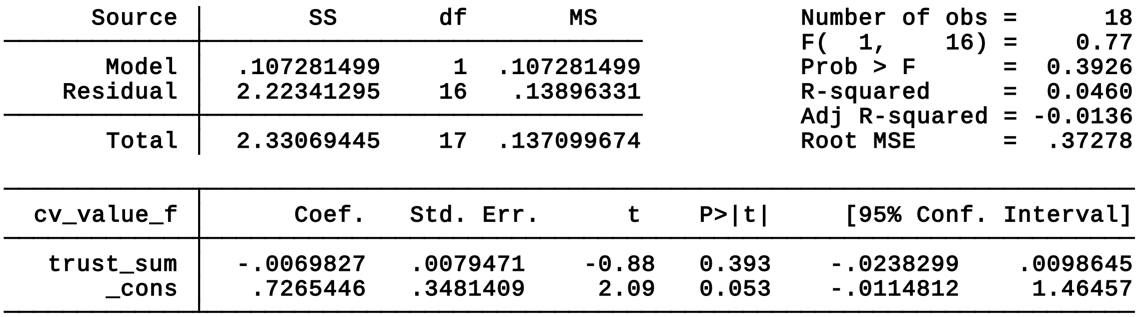
```
                           Number of obs =        236    R-squared     =  0.0051
                           Root MSE      =    .267027    Adj R-squared = -0.0078

               Source │ Partial SS    df       MS           F     Prob > F
   ───────────────────┼──────────────────────────────────────────────────
                Model │  .084745763     3  .028248588       0.40    0.7559
                      │
           firstparty │   .06779661     1   .06779661       0.95    0.3305
             reviewed │  .016949153     1  .016949153       0.24    0.6263
  firstparty#reviewed │  4.8591e-31     1  4.8591e-31       0.00    1.0000
                      │
             Residual │  16.5423729   232  .071303331
   ───────────────────┼──────────────────────────────────────────────────
                Total │  16.6271186   235  .070753696
```

Figure Z - Results from two-way ANOVA of CV_WTP on firstParty and reviewed



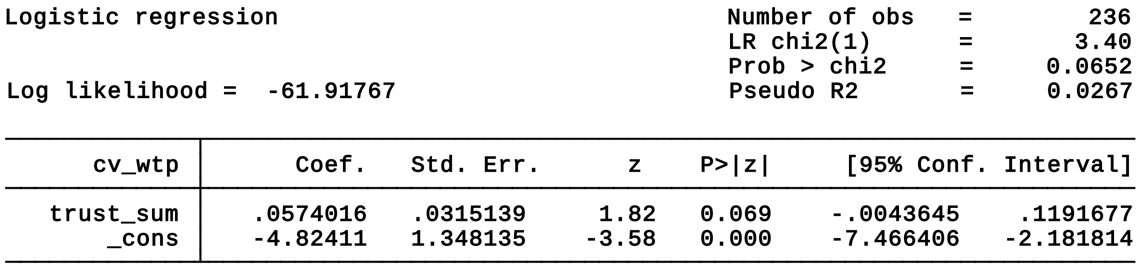
```
      Source │       SS           df       MS      Number of obs   =       236
─────────────┼──────────────────────────────────   F(1, 234)       =      0.31
       Model │  .007115253         1  .007115253   Prob > F        =    0.5794
    Residual │  5.40588269       234  .023102063   R-squared       =    0.0013
─────────────┼──────────────────────────────────   Adj R-squared   =   -0.0030
       Total │  5.41299794       235  .023034034   Root MSE        =    .15199

──────────────────────────────────────────────────────────────────────────────
  cv_value_f │      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
─────────────┼────────────────────────────────────────────────────────────────
   trust_sum │   .0006858   .0012358     0.55   0.579    -.0017489    .0031206
       _cons │   .0060449   .0492836     0.12   0.902    -.0910513    .1031411
──────────────────────────────────────────────────────────────────────────────
```

Figure AA - Results of linear regression of EQ 3 on all respondents



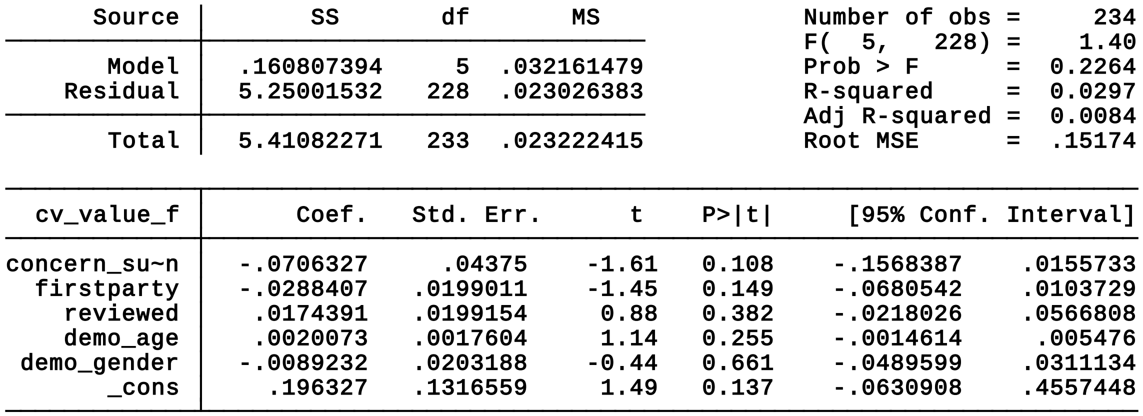
```
      Source │       SS           df       MS      Number of obs   =        18
─────────────┼──────────────────────────────────   F(1, 16)        =      0.77
       Model │  .107281499         1  .107281499   Prob > F        =    0.3926
    Residual │  2.22341295        16   .13896331   R-squared       =    0.0460
─────────────┼──────────────────────────────────   Adj R-squared   =   -0.0136
       Total │  2.33069445        17  .137099674   Root MSE        =    .37278

──────────────────────────────────────────────────────────────────────────────
  cv_value_f │      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
─────────────┼────────────────────────────────────────────────────────────────
   trust_sum │  -.0069827   .0079471    -0.88   0.393    -.0238299    .0098645
       _cons │   .7265446   .3481409     2.09   0.053    -.0114812     1.46457
──────────────────────────────────────────────────────────────────────────────
```

Figure BB - Results of linear regression of EQ 3 on only willing to pay respondents



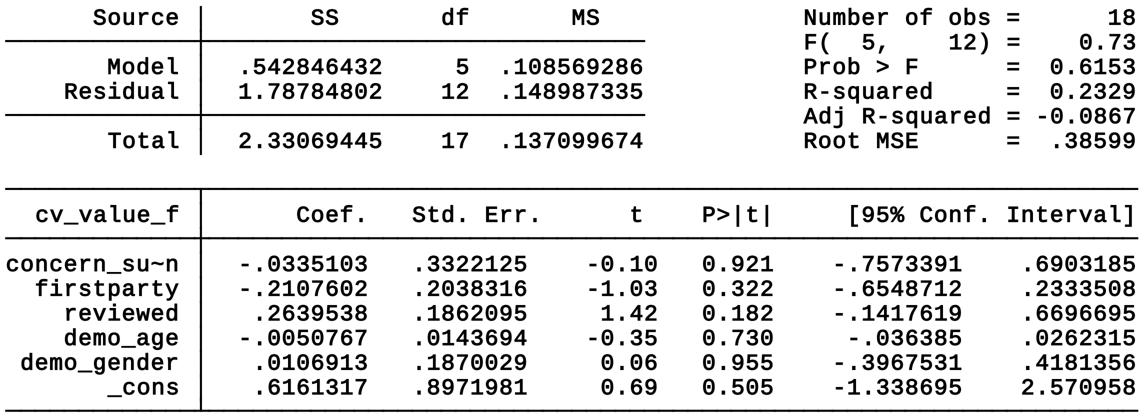
```
Logistic regression                             Number of obs   =        236
                                                LR chi2(1)      =       3.40
                                                Prob > chi2     =     0.0652
Log likelihood =  -61.91767                     Pseudo R2       =     0.0267

------------------------------------------------------------------------------
      cv_wtp |      Coef.   Std. Err.      z    P>|z|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
   trust_sum |   .0574016   .0315139     1.82   0.069    -.0043645    .1191677
       _cons |   -4.82411   1.348135    -3.58   0.000    -7.466406   -2.181814
------------------------------------------------------------------------------
```

Figure CC - Results of logit regression of EQ4 on all respondents



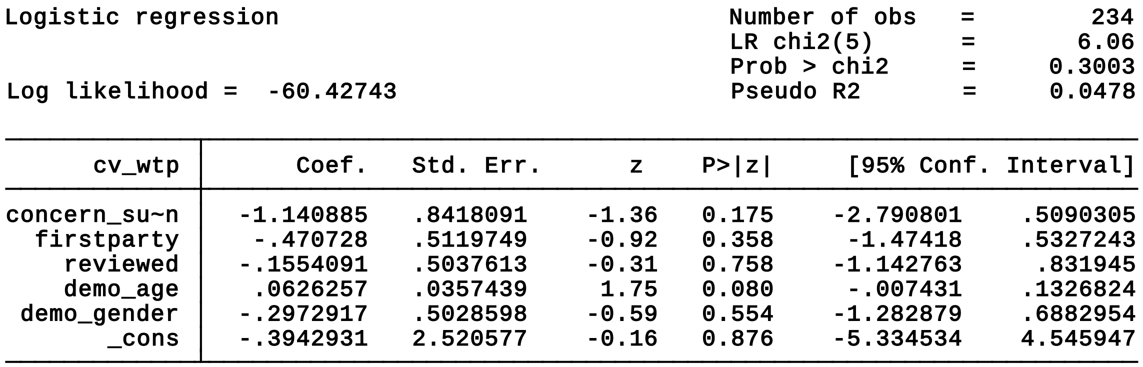
```
      Source |       SS       df       MS              Number of obs =     234
-------------+------------------------------           F(  5,   228) =    1.40
       Model |  .160807394     5  .032161479           Prob > F      =  0.2264
    Residual |  5.25001532   228  .023026383           R-squared     =  0.0297
-------------+------------------------------           Adj R-squared =  0.0084
       Total |  5.41082271   233  .023222415           Root MSE      =  .15174

------------------------------------------------------------------------------
  cv_value_f |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |  -.0706327     .04375    -1.61   0.108    -.1568387    .0155733
  firstparty |  -.0288407   .0199011    -1.45   0.149    -.0680542    .0103729
    reviewed |   .0174391   .0199154     0.88   0.382    -.0218026    .0566808
    demo_age |   .0020073   .0017604     1.14   0.255    -.0014614     .005476
 demo_gender |  -.0089232   .0203188    -0.44   0.661    -.0489599    .0311134
       _cons |    .196327   .1316559     1.49   0.137    -.0630908    .4557448
------------------------------------------------------------------------------
```

Figure DD - Results of linear regression of EQ5 on all respondents



```
      Source |       SS       df       MS              Number of obs =      18
-------------+------------------------------           F(  5,    12) =    0.73
       Model |  .542846432     5  .108569286           Prob > F      =  0.6153
    Residual |  1.78784802    12  .148987335           R-squared     =  0.2329
-------------+------------------------------           Adj R-squared = -0.0867
       Total |  2.33069445    17  .137099674           Root MSE      =  .38599

------------------------------------------------------------------------------
  cv_value_f |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |  -.0335103   .3322125    -0.10   0.921    -.7573391    .6903185
  firstparty |  -.2107602   .2038316    -1.03   0.322    -.6548712    .2333508
    reviewed |   .2639538   .1862095     1.42   0.182    -.1417619    .6696695
    demo_age |  -.0050767   .0143694    -0.35   0.730     -.036385    .0262315
 demo_gender |   .0106913   .1870029     0.06   0.955    -.3967531    .4181356
       _cons |   .6161317   .8971981     0.69   0.505    -1.338695    2.570958
------------------------------------------------------------------------------
```

Figure EE - Results of linear regression on EQ5 on willing to pay respondents



```
Logistic regression                               Number of obs   =        234
                                                  LR chi2(5)      =       6.06
                                                  Prob > chi2     =     0.3003
Log likelihood =  -60.42743                       Pseudo R2       =     0.0478

------------------------------------------------------------------------------
      cv_wtp |      Coef.   Std. Err.      z    P>|z|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
concern_su~n |  -1.140885   .8418091    -1.36   0.175    -2.790801    .5090305
  firstparty |   -.470728   .5119749    -0.92   0.358     -1.47418    .5327243
    reviewed |  -.1554091   .5037613    -0.31   0.758    -1.142763     .831945
    demo_age |   .0626257   .0357439     1.75   0.080     -.007431    .1326824
 demo_gender |  -.2972917   .5028598    -0.59   0.554    -1.282879    .6882954
       _cons |  -.3942931   2.520577    -0.16   0.876    -5.334534    4.545947
------------------------------------------------------------------------------
```

Figure FF - Results of logit regression of EQ6 on all respondents