

University of Mississippi

eGrove

Honors Theses

Honors College (Sally McDonnell Barksdale
Honors College)

Spring 5-2021

Politics of Privacy: The Role of Individual Political Views in Consumer Data Privacy Concerns

Connor Neill

Follow this and additional works at: https://egrove.olemiss.edu/hon_thesis



Part of the [E-Commerce Commons](#), and the [Marketing Commons](#)

Recommended Citation

Neill, Connor, "Politics of Privacy: The Role of Individual Political Views in Consumer Data Privacy Concerns" (2021). *Honors Theses*. 1697.

https://egrove.olemiss.edu/hon_thesis/1697

This Undergraduate Thesis is brought to you for free and open access by the Honors College (Sally McDonnell Barksdale Honors College) at eGrove. It has been accepted for inclusion in Honors Theses by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

POLITICS OF PRIVACY: THE ROLE OF INDIVIDUAL POLITICAL VIEWS IN
CONSUMER DATA PRIVACY CONCERNS

By
Connor Neill

A thesis submitted to the faculty of The University of Mississippi in partial fulfillment of the
requirements of the Sally McDonnell Barksdale Honors College.

Oxford, MS
May 2021

Approved By

Advisor: Dr. Melissa Cinelli

Reader: Dr. Christopher Newman

Reader: Dr. Gary Hunter

© 2021

Connor Nicole Neill

ALL RIGHTS RESERVED

DEDICATION

To my family, both in Texas and at Ole Miss, who have been there every step of the way.

Hotty Toddy and Hook'em Horns.

ACKNOWLEDGEMENTS

I would like to thank my parents and my sister for always cheering me on and challenging me to be my best. I would not have been able to juggle this research, a small business, and my senior year without your help. Thank you for allowing me to explore the world and chase my dreams.

I would also like to thank Dr. Melissa Cinelli for being my fearless guide and mentor on this research journey in a very chaotic year, I would have been lost without you. As well as to all the faculty in the Marketing, Management Information Systems and Accounting Departments and the Sally McDonnell Barksdale Honors College, thank you for encouraging me to forge my own path on this campus and beyond.

And a special thank you to the School of Business Administration and the University Study Abroad Office whose 2019 August Intercession program in Dublin, Ireland was the initial inspiration for this research topic.

ABSTRACT

Today, every choice that is made, from where to shop to what music to listen to, has turned into a reflection of one's political views and identity. The main purpose of this research is to explore the relationship between an individual's political views and his or hers attitudes toward the security of personal information in the consumer realm. Two studies were conducted in the form of surveys. The first study aims to measure the consumer's trust and risk beliefs for a company of a certain size as well as their feelings toward the dimensions of control, collection, and awareness of privacy practices. The second study focuses on consumer attitudes and behaviors post-data breach, again taking into account the size of the firm, as well as their repatronage intentions and beliefs about improper access. Both studies were analyzed with the individual consumer's political views as a main effect. It was found that political views did not affect how consumers felt about control, collection and awareness beliefs. Risk beliefs were found to be a mediator between political views and intention to reveal information for liberal and extremely conservative consumers. No significant findings for the role of political orientation or firm size in the consumer beliefs and attitudes came from the second study.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS	vi
INTRODUCTION	1
CHAPTER II: OVERVIEW OF POLITICS & THE CONSUMER	3
CHAPTER I: REVIEW OF INFORMATION PRIVACY SCALES	8
CHAPTER III: STUDY 1 – POLITICAL VIEWS & PRIVACY CONCERNS	12
CHAPTER IV: STUDY 2 – POLITICAL VIEWS & DATA BREACH	19
CONCLUSION	23
REFERENCES	26
APPENDIX A: STUDY 1	31
APPENDIX B: STUDY 2	46

LIST OF ABBREVIATIONS

CFIP	Concern for information privacy
DATA	Data Accountability and Trust Act of 2009
GIPC	Global information privacy concern
IUIPC	Internet users' information privacy concerns
SECS	Social and Economic Conservatism Scale

INTRODUCTION

Over the last 20 years, the world has become increasingly digital. As individual's lives, both personal and consumer, continue to move further into the digital realm, there has also been an increase in concerns for the privacy of their personal data. It is almost impossible for consumers to get through a day without a business or other organization asking for or collecting information about them. In previous literature, consumer privacy has been defined as:

“the consumer's ability to control (a) presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present” (Goodwin 1991).

This definition is based on two elements of control including control over who has access to collect information, specifically when the interaction is unwanted, and what information they collect during those interactions. Control is central to consumer information privacy concerns. Previous literature has identified that consumer privacy concerns are influenced by other factors that go beyond the dimension of control including their awareness of information collection and usage, the sensitivity of that information and familiarity with the entity (Sheehan and Hoy 2000). This study will aim to explore to influence of familiarity with the entity through the manipulation of firm size in a hypothetical shopping scenario.

Examples of the type of information that would be considered consumer information that would be at the center of these concerns include demographic, search history and personal

profile information (Martin and Murphy 2017). More importantly consumers are concerned about the security of their personally identifying information including their full name and address in combination with their financial information; this type of information is central to major data privacy laws in the United States such as the Data Accountability and Trust Act of 2009.

Because this information is so sensitive, sharing it with companies can cause a consumer to feel vulnerable. This vulnerability stems from the potential for harm resulting from a data breach, but not necessarily the actual misuse of their information (Scharf 2007). It is important to understand how a data breach affects consumer perceptions of a company and the effects it will have on future consumer behaviors. Previous research has found that customer control and company transparency can work together to mitigate negative post-data breach behaviors (Martin, Borah and Palmatier 2017). While beliefs on control and awareness of privacy practices are key dimensions in measuring consumer data privacy concerns, one study found that data privacy concerns were not a predictor of negative customer behavior outcomes (Martin, Borah and Palmatier 2017).

Our world has also become more politically motivated and influenced in recent years. It can be seen without conducting research, that politics have seeped into almost every aspect of our lives. Research has established political beliefs are connected to an individual's underlying needs and motivations, and thus creating cognitive difference between conservative and liberal individuals (Jost et al 2003). It has also been found that an individual's political views do play a role in their decisions as a consumer (Carney et al 2008). It is reasonable to assume that these cognitive differences will also affect their data privacy concerns.

CHAPTER I: OVERVIEW OF POLITICS & THE CONSUMER

CONSERVATIVE VS LIBERAL CONSUMERS

As mentioned earlier, there are distinct cognitive differences among individuals with liberal and conservative political views. In this section we will dive deeper into those characteristics that are most relevant to the realm of data privacy. Conservatives are characterized as avoiding uncertainty and mitigating threats (Jost et al 2003). However, it has also been found that conservatives are more likely to take financial risks than liberals, but not in other areas of life (Choma et al 2013). In the greater context of the consumer journey, conservatives are less likely to conduct information search or switch brands; they were also found to have an affinity for national brands rather than generic brands (Jung and Mittal 2020). When these characteristics are applied in the context of data privacy concerns one might infer that conservative consumers would have stronger beliefs around control because of their intolerance of uncertainty as well as being more trusting of larger companies.

In terms of post-consumption behaviors, research has found that conservatives are less likely to issue complaints or dispute resolutions from companies than liberals (Jung et al 2017). The same research shared that this happens because of conservatives' high system-justification motivation, which makes them more accepting of the current state of things (Jung et al 2017). In a related way, previous literature was found that liberals express more happiness, while conservatives perceive to feel more happiness (Napier and Jost 2008, Wojcik et al 2015). With

these characteristics in mind, conservatives and liberals are likely to react differently when the security of their personal information is threatened or compromised.

POLITICAL PARTIES STANCE ON DATA PRIVACY

To compare the stance of the major political parties, Republican and Democrat, on the issue of consumer data privacy, each party's most recent platform from their respective national committee was reviewed.

The Democratic National Committee had a subsection under their economic platform dedicated to consumer rights and privacy. This is an excerpt taken from that section:

“In the 21st century...it is all but impossible for consumers, students, workers, and people with disabilities to opt out of using the internet to shop, socialize, learn, work, bank, and live. Democrats are committed to policies that will protect individuals' privacy and data rights while continuing to support and enable innovation and improve accessibility in the technology sector” (2020 Democratic Party Platform, 2020, p. 25).

They then go on to mention legislation that the future, now current, administration plan to update to better fit today's consumer environment; namely, the Obama Administration's “Consumer Privacy Bill of Rights” and the “Electronic Communications Privacy Act” from the 1980s.

The Republican National Committee's stance on consumer privacy concerns is not as clear cut, but they do address the topic in the section “The Fourth Amendment: Liberty and Privacy”. The evolution of data encryption technology is mentioned, stating “privacy protections have become crucial to the digital economy” (Republican Platform 2020, 2020, p. 13). While there is no mention of future legislative action, the sentiment is present.

One monumental piece of legislation surrounding information privacy concerns is the Data Accountability and Trust Act of 2009 (DATA). The purpose of this act was “to protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach” (Data Accountability and Trust Act of 2009, 2009). It also defines what is considered to be “personally identifying information”; this includes an individual’s first and last name, home address and phone number combined with their Social Security Number, government identification number or financial account information. This would cover any information that a consumer would give to an online retailer when purchasing a good or service. When this act was introduced, it was sponsored by Representative Rush of Illinois (D), but was co-sponsored by four other Representatives, three of which were Republicans.

While the party’s most recent platforms may differ in level of acknowledgement, in terms of recent legislation, both Republicans and Democrats have consumer data privacy concerns on their mind. We will briefly discuss two different bills that were introduced to the 116th Congress. The first being the “Consumer Online Privacy Rights Act” introduced by Senator Cantwell (D) of Washington; it was co-sponsored by three other Democrats. This bill would require companies that process or transfer consumer data to have public and readily accessible privacy policies as well as have designated privacy and data security officers. There are also provisions that prohibit these companies from engaging in ill-mannered data practices such as sharing data without affirmative consent or to an unreasonable point past the consent received. In order to enforce these, the Federal Trade Commission would need to establish a new bureau (Consumer Online Privacy Rights Act, 2019). A similar bill was introduced in the second session entitled “Consumer Data Privacy and Security Act of 2020” by Senator Moran of Kansas (R). The topics

of this bill include an overview of the collection process, a consumer's right to awareness of privacy practices and their control over their personal information (Consumer Data Privacy and Security Act of 2020, 2020). After looking at these proposed bills alone, it is evident that, while each party's specific approach to the issue may be different, the topic of consumer data privacy is relevant today. It may also be important to note the sponsors of each bill; there has never been a strong division about Republicans and Democrats on whether consumer privacy is an issue in this country, but there has been a shift away from bipartisanship in the authoring and sponsoring of bills surrounding this topic.

REVIEW OF POLITICAL SCALE USED

There are many ways that political identity can be measured. A single-item measure such as party affiliation or how an individual voted in a recent election could be used. It is important to acknowledge that an individual's political views are separate from their party affiliation, though their party may be a sign of their actual political identity. Other observable behaviors such as what channel consumers receive their news from can be an indication of political views (Mitchell et al 2014). Multi-item scales are seen to be highly reliable as they take into account more than one measure, but if the statements are slanted in any way, they can create response bias.

In these studies a 12-item scale measuring the level of positive or negative attitude an individual has toward a series of social and economic political issues will be used (Everett 2013). This scale, known as the Social and Economic Conservatism Scale, was developed in order to efficiently and effectively measure an individual's attitudes toward "peripheral" aspects of conservatism. The items included on the scale are as follows: abortion, the family unit, religion, traditional marriage, traditional values, patriotism, military and national security, fiscal

responsibility, business, limited government, gun ownership and welfare benefits (Everett 2013).

When developed, it was found that the measure of conservatism on the SECS was highly correlated with self-reported political affiliations, supporting this scale as an accurate way to measure an individual's views.

CHAPTER II: REVIEW OF INFORMATION PRIVACY SCALES

GIPC & CFIP

A one-dimensional theoretical framework, referred to as a global information privacy concern (GIPC) scale, for measuring information privacy concerns was replaced by a multidimensional scale in the late nineties. Consumer information privacy concerns have become more and more complex with the introduction of new technology and new methods of data collection. Smith et al. (1996) created this new scale called the concern for information privacy (CFIP) scale because the GIPC scale measured individual's concerns but did not dive into the dimensions that made up that concern.

The CFIP scale can be broken down into four subscales based on the following dimensions: collection, errors, unauthorized secondary use, and improper access. Collection can be defined as the “concern that extensive amounts of personally identifiable data are being collected and stored in databases” (Smith et al, 1996). Errors refer to the “concern that protections against deliberate and accidental errors in personal data are inadequate” (Smith et al, 1996). Smith et al, further broke down the dimension of unauthorized secondary use into internal use by the collection organization and external use by another party (1996); in the end, it was determined that unauthorized use could be measured as one. The final dimension in the CFIP scale is improper access, referring to the “concern that data about individuals are readily available to people not properly authorized to view or work with this data” (Smith et al, 1996).

Individuals were presented with a series of fifteen statements related to information privacy concerns and then asked the extent to which they agree with those statements using a

seven-point Likert scale ranging from “Strongly disagree” to “Strongly agree”. Questions regarding possible causal variables, individual factors and behavioral intentions were included to assess nomological validity. The antecedents in question were the frequency of experiencing an “invasion of privacy” and the frequency of exposure to literature and media surrounding the misuse of information; these were measured on Likert scales as well (Smith et al 1996). The individual factors explored were those of trust/distrust, paranoia, and social criticism; it was thought that these factors were positively correlated with an individual’s information privacy concerns and the results support that hypothesis. These were measured using previously developed scales. According to research done by Stone et al (1983), it is likely that individuals with a high level of concern for the privacy and security of their personal information will be hesitant or refuse to give that information in the future. Smith’s study found strong support for this statement as well.

It is important to note that Smith et al (1996) found that the greatest concern amongst individuals surrounded the improper use of their personal information, as opposed to concerns over control, collection, and errors. Improper use of information is the dimension that consumers have the least amount of direct influence over. Companies are likely to act in an opportunistic manner when given the chance, making sharing personal information a risky behavior in the eyes of the consumer thus heightening their concern (Milne and Gordon 1993, Laufer and Wolf 1997). Individuals can, to an extent, determine who collects their information, how much and what type of information is collected and the accuracy of that information, but once it is collected, the consumer has little sway over how the company uses it.

IUIPC

As the Internet continued to become central to the consumer information collection process, an updated scale for the measurement of information privacy concerns amongst Internet users was needed. The Internet Users' Information Privacy Concerns (IUIPC) scale was developed around three factors: collection, control, and awareness of privacy practices (Malhotra et al 2004). These dimensions have their roots in social contract theory (Donaldson and Dunfee 1994). Social contract theory in the context of information privacy concerns is this way:

“a firm's *collection* of personally identifiable data is perceived to be fair only when the consumer is granted *control* over the information and the consumer is *informed* about the firm's intended use of the information” (Malhotra et al 2004, p 339).

The dimensions of collection and control in IUIPC were also present in CFIP; these measures were adapted from CFIP to fit Internet marketing as opposed to traditional marketing. Awareness of privacy practices relates to the dimensions of unauthorized secondary use and improper access, it has a narrower focus on the concern surrounding organizational practices (Malhotra et al 2004). Knowing how the company is using consumer data is just as important as, if not even more telling, than knowing what a company is not going to allow happen to an individual's data.

In addition to measuring these three dimensions, Malhotra et al (2004) developed a causal model to describe how IUIPC is connected to a consumer's sharing, or lack thereof, of information in certain scenarios, more specifically when the level of sensitivity of the information varies; this is based on the knowledge that privacy threats are dependent on the type of information shared (Phelps et al. 2000, Sheehan and Hoy 2000). This causal model was based on trusting and risk beliefs, which have been determined to be the most important beliefs in the context of

information privacy concerns (Cespedes and Smith 1993, Miyazaki and Fernandez 2000, Sheehan and Hoy 2000). Trusting beliefs can be defined as how dependable consumers perceive a company to be with the security of their data (Grazioli and Jarvenpaa 2000); risk beliefs are defined as the consumer's perception of potential loss associated with sharing their information (Dowling and Staelin 1994).

The original study done with the IUIPC scale and related causal model found that an inverse relationship exists between privacy concerns and trusting beliefs as well as between the sensitivity of information and those same beliefs. This means that as privacy concerns increased, trusting beliefs were lowered; similarly, as marketers asked for more sensitive information, the consumer's trusting beliefs decreased. A positive relationship was found to exist between consumer trusting beliefs and their intention to share information, while an inverse relationship existed between information sensitivity and intention to share (Malhotra et al 2004). One of the biggest takeaways from the Malhotra (2004) study is that online consumers are most concerned with being aware of and having direct control over their information. The results of the study established IUIPC scale as an efficient and effective way to measure information privacy concerns among online consumers. These previously established information privacy scales will be the foundation of this study.

CHAPTER III: STUDY 1 – POLITICAL VIEWS & PRIVACY CONCERNS

HYPOTHESES

It has been established that there are cognitive differences between those with conservative and liberal political views, thus effecting their consumer decision making process.

Within the context of consumer data privacy concerns, it is hypothesized that:

H1: Political orientation affects consumer beliefs about control over and collection of personal information.

H1a: Conservative political views will have a positive effect on consumer control and collection beliefs.

H1b: Consumers with liberal and conservative views will have similar beliefs about awareness of privacy practices.

Previous literature has determined that company size can be a signal for consumers that a firm can be trusted. This can be contributed to seeing a large number of other consumers engaging with this company or the understanding that larger firms are likely to have more resources and stronger procedures in place (Doney and Cannon 1997, Chow and Holden 1997). Another element of perceived firm size that signals to consumers that they can be trusted is the notion that a larger company has more to lose by acting in an untrustworthy or unethical way (Jarvenpaa, Tractinsky and Vitale 2000). For this reason, a portion of this study measures an

individual's trusting and risk beliefs for a store, either small or large, requesting access to personal information.

H2: Company size affects consumer trusting and risk beliefs and intention to share.

H2a: Company size will have a positive effect on trusting beliefs and intention to share.

H2b: Company size will have a negative effect on risk beliefs.

With all of this being said, it is hypothesized that an individual's political views will interact with their perceptions of a company based on size in the follow way:

H3: Consumer political views and company size interactively affect consumer trusting and risk beliefs and intention to share.

H3a: Consumers with liberal political views will have higher trusting beliefs when the company size is small.

H3b: Consumers with conservative political views will have similar levels of trusting and risk beliefs regardless company size.

METHODS

The study was administered in the form of a survey through mTurk with a sample size of 159 adults in the United States. Consumers' attitudes and beliefs toward data privacy concerns on the dimensions of control, collection and awareness of privacy practices were measured as done in IUIPC (Malhotra et al 2004) and CFIP adapted for the Internet (Smith et al 1996). Political views were measured using the 12-item SECS (Everett 2013), as well as directly asked for in the form of political party affiliation. When scoring this scale, 0 was conservative and 100 was liberal.

One of two hypothetical shopping scenarios were shown to participants: one involving a small, local retailer and the other being large and national retailer. In the scenario, the retailer was asking for the full name, address, and credit card information of the consumer for a membership to gain access to special pricing and other deals. A series of questions regarding trusting and risk beliefs associated with these scenarios; these were adapted from the causal model developed by Malhotra et al (2004). These were each measured on a 7-point Likert scale with anchors of *Strongly Disagree* and *Strongly Agree*. The customer's intention to share their information with the respective company was also measured on a 7-point Likert scale. The anchors for this scale were *Unlikely to Likely*, *Not Probable to Probable*, and *Unwilling to Willing*.

Other behaviors involving consumer information were measured including online shopping habits and obtaining credit/debit cards through retailers. Measures for gender, age, income and education level were also taken.

RESULTS

Prior to analysis, the three items measuring likelihood to provide personal information to the firm were averaged to form a single item ($\alpha = 0.98$). Similarly, the four items measuring trust beliefs were averaged to form a single item ($\alpha = 0.91$) and the four items measuring risk beliefs were averaged to form a single item ($\alpha = 0.93$).

H1, including H1a and H1b, predicted that political orientation would have an effect on the three foundational dimensions of consumer information privacy concerns. To test for these for the relationships, a regression model was used with the attitudes toward the dimensions as the dependent variable and the individual's political views (0= Very Conservative to 100 = Very

Liberal) as the independent variable. It was determined that no relationship exists between the information privacy dimensions of control ($t=-.291$, $p=.772$) or collection ($t=-.554$, $p=.580$) and political orientation. No relationship was found between individual political views and awareness of privacy practices either ($t=-.799$, $p=.426$).

H2, including H2a and H2b, predicted that company size would have an effect on consumer trust and risk beliefs as well as their intention to reveal information. To test H2a for consumer trust beliefs, PROCESS Model 1 was used with 5,000 bootstrap samples (Hayes 2018). Firm size (0 = small, local; 1 = large, national) and political orientation (0 = very conservative to 100 = very liberal; mean-centered prior to analysis [Aiken and West 1991]) were entered as independent variables and measure of trust beliefs was entered as the dependent variable. There was no effect of firm size ($t = 0.61$, $p = 0.54$) or political views ($t = -1.18$, $p = .24$), or firm size by political orientation interaction ($t = 1.59$, $p = .11$).

To test H2b regarding consumer risk beliefs, PROCESS Model 1 was used with 5,000 bootstrap samples (Hayes 2018). Firm size (0 = small, local; 1 = large, national) and political orientation (0 = very conservative to 100 = very liberal; mean-centered prior to analysis [Aiken and West 1991]) were entered as independent variables and measure of risk beliefs was entered as the dependent variable. There were no main effects of either company size ($t = -1.24$, $p = .22$) or political orientation ($t = -0.27$, $p = .78$), but, consistent with H3, there was a significant firm size by political orientation interaction ($t = -3.12$, $p = .002$). The Johnson-Neyman technique (Johnson and Neyman 1936) was used to highlight the regions in which the moderating effect of political orientation on the relationship between firm size and risk beliefs was significant. The analysis reveals that at the very low end of the political orientation scale (values < 12.05), corresponding to very conservative political beliefs, respondents believed providing information

to small firms was less risky than providing information to large firms ($ps < .05$). Conversely, among respondents at the middle and high ends of the political orientation scale (values > 45.99), providing information to large firms was perceived to be less risky than providing information to small firms ($ps < .05$).

To test H2a for intention to share personal information, PROCESS Model 1 was used with 5,000 bootstrap samples (Hayes 2018). Firm size (0 = small, local; 1 = large, national) and political orientation (0 = very conservative to 100 = very liberal) were entered as independent variables [mean-centered prior to analysis (Aiken and West 1991)] and willingness to provide information (1 = Not at all Willing to 7 = Very Willing) was entered as the dependent variable. There were no main effects of firm size ($t = 0.41$, $p = .68$) or political orientation ($t = .26$, $p = .79$). The analysis revealed only the predicted firm size by political orientation interaction ($t=2.28$, $p=.024$). The Johnson-Neyman technique (Johnson and Neyman 1936) was used to highlight the regions in which the moderating effect of political orientation on the relationship between firm size and willingness to provide information was significant. The analysis reveals that at the low end of the political orientation scale (corresponding to conservative political beliefs), firm size did not influence respondents' willingness to provide information; the interaction did approach significance at the very bottom of the scale (values < 9.90). However, as respondents became more liberal in their political orientation (values > 62.09), respondents became increasingly more willing to provide information to larger firms than to smaller firms ($ps < .05$).

To test for moderated mediation, PROCESS Model 8 was used with 5,000 bootstrap samples (Hayes 2018). Specifically, this analysis tested whether firm size and political orientation interactively affected willingness to provide information due to beliefs about the

riskiness of providing such information. Firm size (0 = small, 1 = large), political orientation (0 = very conservative, 100 = very liberal), and their interaction were predictor variables, risk beliefs were the mediator, and willingness to provide information was the dependent variable. All predictor variables were mean-centered prior to analysis. The analysis revealed that political orientation does moderate the indirect effect of firm size on willingness to provide information through risk beliefs (*Index of Moderated Mediation*: .0091, .0581). Specifically, the indirect effect was significant among relatively more liberal respondents (+1 SD; IE = .86, CI: .26, 1.47) but not among those at the mean of the political orientation scale (IE = .24, CI: -.15, .66) or those relatively more conservative (-1 SD; IE = -.38, CI: -1.03, .24).

DISCUSSION

For the most central dimensions of consumer privacy concerns, there is no relationship with individual political views. This supports H1b hypothesizing liberals and conservatives would respond similarly for awareness beliefs, but does not support H1a regarding control and collection beliefs. This can be seen not only in the data, but also in the inclusion of privacy concerns in recent legislation for both major political parties in the United States. Consumers across the spectrum of political views find having control over the collection of their data as well as being aware of how companies are using this data to be important issues. For companies this means that they must continue to create transparency in their privacy practices because it is likely that most, if not all, their consumers have some level of concern for the security of their data.

Previous literature, as referenced earlier in this paper, found that larger companies were perceived as more trustworthy by consumers. Company size alone was not found to effect consumer trust and risk beliefs or their willingness to share their information, but when the

variable of political views is added then a pattern emerges. When a consumer fell within a certain level of political orientation on a scale from 0 to 100 there was a significant effect on their risk beliefs depending on the size of the firm. For those measuring very low on the scale, meaning they could be considered extremely conservative, perceived less risk when the firm was small. When the consumer was a moderate or liberal, there was less perceived risk when the company was large. These findings go against the stereotypical idea of conservatives supporting “big business” and liberals being against it. Consistent with the low levels of perceived risk, it was found that consumers measuring more liberal on the scale were more willing to provide their personal information when the company was large. Again, this does not align with the typical idea of the types of business a liberal might frequent.

A mediation model was found such that an individual’s political beliefs moderate the indirect effect of company size on the consumer’s willingness to reveal information through their risk beliefs about that company. This means that political orientation affects how size influences risk beliefs which then determine the consumer’s intention to share. This mediation is most prevalent among liberal consumers, similar to the effects found in earlier hypotheses discussion. This triangular relationship will be important for companies to consider when implementing privacy policies.

CHAPTER IV: STUDY 2 – POLITICAL VIEWS & DATA BREACH

HYPOTHESES

Knowing that size has been shown to affect customer perceptions of a store and thus effect their consumer behaviors, the following is hypothesized about the relationship between company size and consumer attitudes after a data breach:

H4: Company size will affect consumer attitude toward the company after a data breach, their likelihood of returning and their beliefs about improper access.

H4a: Company size will have a positive effect on consumer attitude toward the company after a data breach and on likelihood of returning.

H4b: Company size will have a negative effect on consumer beliefs about improper access to consumer data.

Political views have been found to be linked to how individuals express their emotions, both in life satisfaction and consumer satisfaction. To that end, it is likely that an individual's political views will play a role in their attitudes and beliefs about a company post-data breach.

H5: Consumer political views will affect consumer attitudes toward the company after a data breach, their likelihood of returning and their beliefs about improper access.

H5a: Consumers with conservative political views will have more positive attitudes toward a company after a data breach and will also have a higher likelihood of returning.

H5b: Consumers with conservative and liberal political views will have similar beliefs about improper access.

Similarly to Study 1, it is hypothesized that these two variables, political views and company size, will interact with one another.

H6: Consumer political views and company size interactively affect consumer attitudes toward the company after a data breach, their likelihood of returning and their beliefs about improper access.

H6a: Consumers with conservative political views will have a higher intention to return when the company is large.

H6b: Consumers with liberal political views will have a more positive attitude toward a company after a data breach despite when the firm is small.

H6c: Consumers with conservative and liberal political views will have similar beliefs about improper access when the company is large, but liberals will have more positive beliefs when the company is small.

METHODS

The study was administered in the form of a survey through mTurk with a sample size of 142 adults in the United States. One of two hypothetical shopping scenarios were shown to participants: one involving a small, local retailer and the other being large and national retailer. In the scenario, the retailer was asking for the full name, address, and credit card information of the consumer for a membership to gain access to special pricing and other deals. Participants were then asked to imagine that after 6 months of enjoying the membership, a data breach

occurred at the company and their personal information was compromised. A series of questions surrounding consumers attitudes toward the company post-data breach associated with these scenarios as well as the consumer's intention to give their personal information again were asked. Questions about improper access beliefs adapted from Smith et al (1996) were also included.

Participants were asked about their frequency of falsifying information as well as a measure of potential breach as a motive for these actions. Other behaviors involving consumer information were measured including online shopping habits and obtaining credit/debit cards through retailers. These measures went beyond those of Study 1 by asking about post-data breach behaviors in these situations as well. Measures for gender, age, income and education level were also taken.

RESULTS

Prior to analysis, the three items measuring retailer attitude were averaged to form a single item ($\alpha = 0.94$). The two items measuring repatronage intentions were averaged to form a single item ($r = 0.94$). The three items measuring beliefs about improper access (Malholtra 2004) were averaged to form a single item ($\alpha = 0.68$).

To test H4-H6 for consumer attitude toward the company post-data breach, PROCESS Model 1 was used with 5,000 bootstrap samples (Hayes 2018). Firm size (0 = small, local; 1 = large, national) and political orientation (0 = very conservative to 100 = very liberal; mean-centered prior to analysis [Aiken and West 1991]) were entered as independent variables and measure of attitude was entered as the dependent variable. There was no effect of firm size (t

=.64, $p = .52$) or political views found ($t = .24$, $p = .81$), or firm size by political orientation interaction ($t = -.14$, $p = .89$).

To test H4-H6 for consumer repatronage intention post-data breach, PROCESS Model 1 was used with 5,000 bootstrap samples (Hayes 2018). Firm size (0 = small, local; 1 = large, national) and political orientation (0 = very conservative to 100 = very liberal; mean-centered prior to analysis [Aiken and West 1991]) were entered as independent variables and measure of likelihood to return to this company was entered as the dependent variable. There was no effect of firm size ($t = 1.49$, $p = .14$) or political views found ($t = .19$, $p = .85$), or firm size by political orientation interaction ($t = .32$, $p = .75$).

To test H4-H6 for consumer beliefs about improper access post-data breach, PROCESS Model 1 was used with 5,000 bootstrap samples (Hayes 2018). Firm size (0 = small, local; 1 = large, national) and political orientation (0 = very conservative to 100 = very liberal; mean-centered prior to analysis [Aiken and West 1991]) were entered as independent variables and measure of likelihood to return to this company was entered as the dependent variable. There was no effect of firm size ($t = -.41$, $p = .68$) or political views found ($t = -.203$, $p = .84$), or firm size by political orientation interaction ($t = -.49$, $p = .62$).

DISCUSSION

While no significant findings came from this second study (no support for H4, H5, or H6), there is still something to be learned from this. If a company experiences a data security breach, it does not matter what market they are in or what size their company is, they will need to pay attention to the attitudes and behaviors of their individual customers because it is unlikely that they will be able to predict consumer behavior without looking at the larger picture.

CONCLUSION

LIMITATIONS

These studies only offered a limited measure of the individual's political views focusing on their social and economic opinions. A more comprehensive political scale might provide greater insight and perhaps even affect the findings of this research. Participants while almost evenly split between measuring as conservative or liberal on the SECS with a median around 42, overwhelmingly identified as members of the Democratic party. This could have been influenced by the timing of this study, coming soon after an extremely high stakes presidential election.

Another limitation, specifically for the second study, is the pallidness of the hypothetical shopping scenario. The lack of vividness for the participant may have affected their reaction to the data breach; There was no direct potential for harm or loss in the study creating less vulnerability in the consumer. If this study were to be re-done, having the participant provide some of their personal information if they determined the company to be trustworthy and then informing them that their data had been stolen would create a different response environment.

FURTHER RESEARCH

Further research might move the shopping scenario into the brick-and-mortar store to see if company size would become more influential. This more traditional shopping scenario might include filling out a card for a giveaway with personally identifying information or a customer profile that goes beyond shopping preferences. This study would be most effective if administered in person to create a more realistic response environment.

Adding the variable of information sensitivity would be another way to expand on this research. The participant could be asked a higher level of sensitive information on each screen seeing if a threshold exists for their intention to share, both online and in person.

Many of the results of this research were opposite of the proposed hypotheses. A mediation model was identified in Study 1, but this does not fully explain why these responses occurred. The most surprising result, in my opinion, was that liberals were more trusting of large companies as that does not follow the stereotype of a Democrat. Adding a qualitative research element allowing participants to elaborate on their feelings toward each company would provide greater insight.

There is a relationship to be explored between political orientation and age in the context of data privacy concerns. When manipulating the data during analysis a trend was spotted amongst older liberal consumers and their beliefs. This generational gap in conjunction with politics is likely to affect other consumer behaviors.

MANAGERIAL IMPLICATIONS

If not already a consideration, managers need to take into account the political orientation of their target market and current customer base when developing and communicating data privacy practices and information collection protocols. Obviously, these policies are enterprise wide and not on a regional or case by case basis, but the way in which the marketing department presents the intended use and handling of requested personal to different markets can vary.

For example, despite popular belief conservatives were found to be less trusting of big business; so a large company might want to dedicate time and effort into building community relationships or being more specific regarding the intended use of the requested personal information at the point of collection in more politically conservative markets to work toward gaining their trust. Similarly, for small companies in more liberal markets, an increase in efforts to mitigate perceived risk among its customers might be needed. This study does not know why conservatives and liberals perceived different levels of risk among small and large companies, so these suggestions might not hold true until the underlying causes are researched further, but the sentiment remains.

An overall recommendation for small businesses, particularly in liberal markets but in moderate markets as well, is to take consumer privacy seriously. Even if not required by law, it is recommended that small business follow the lead of large, national companies when it comes to privacy policies. Having a clear and concise privacy policy that is easily accessible on the company website would help to relieve any hesitations the consumer may have. Findings from this study combined with previous research can establish that control over their data is important to all consumers. By providing a straightforward breakdown of how information is collected, used and protected from misuse, a company can build a strong foundation based on trust with their customer base.

REFERENCES

- 2020 Democratic Party Platform. (2020) from <https://democrats.org/wp-content/uploads/sites/2/2020/08/2020-Democratic-Party-Platform.pdf>.
- Aiken, L. S., West, S. G., & Reno, R. R. (1991). *Multiple regression: Testing and interpreting interactions*. sage.
- Carney, D. R., Jost, J. T., Gosling, S. D., & Potter, J. (2008). The secret lives of liberals and conservatives: Personality profiles, interaction styles, and the things they leave behind. *Political Psychology*, 29(6), 807-840.
- Cespedes, F. V., & Smith, H. J. (1993). Database marketing: New rules for policy and practice. *MIT Sloan Management Review*, 34(4), 7.
- Choma, B. L., Hanoch, Y., Gummerum, M., & Hodson, G. (2013). Relations between risk perceptions and socio-political ideology are domain-and ideology-dependent. *Personality and Individual Differences*, 54(1), 29-34.
- Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020).
<https://www.congress.gov/bill/116th-congress/senate-bill/3456>
- Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).
<https://www.congress.gov/bill/116th-congress/senate-bill/2968>
- Data Accountability and Trust Act of 2009, H.R.2221, 111th Cong. (2009).
<https://www.congress.gov/bill/111th-congress/house-bill/2221>

- Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of management review*, 19(2), 252-284.
- Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. *Journal of marketing*, 61(2), 35-51.
- Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. *Journal of marketing*, 61(2), 35-51.
- Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of consumer research*, 21(1), 119-134.
- Everett, J. A. (2013). The 12 item social and economic conservatism scale (SECS). *PloS one*, 8(12), e82131.
- Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 10(1), 149-166.
- Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 30(4), 395-410.
- Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford publications.
- Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information technology and management*, 1(1), 45-71.
- Jost, J. T., Glaser, J., Kruglanski, A. W., & Sulloway, F. J. (2003). Political conservatism as motivated social cognition. *Psychological bulletin*, 129(3), 339.

- Jung, J., & Mittal, V. (2020). Political identity and the consumer journey: A research review. *Journal of Retailing*, 96(1), 55-73.
- Jung, K., Garbarino, E., Briley, D. A., & Wynhausen, J. (2017). Blue and red voices: Effects of political ideology on consumers' complaining and disputing behavior. *Journal of Consumer Research*, 44(3), 477-499.
- Johnson, P. O., & Neyman, J. (1936). Tests of certain linear hypotheses and their application to some educational problems. *Statistical research memoirs*.
- Laufer, R.S. and Wolfe, M. (1977), Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, 33: 22-42.
- MacKenzie, S. B., & Spreng, R. A. (1992). How does motivation moderate the impact of central and peripheral processing on brand attitudes and intentions?. *Journal of consumer research*, 18(4), 519-529.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), 336-355.
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135-155.
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58.

- Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 12(2), 206-215.
- Mitchell, A., Gottfried, J., Kiley J., & Masta, K.E. (2014, October 21). *Political Polarization & Media Habits*. Pew Research Center: Journalism & Media.
<https://www.journalism.org/2014/10/21/political-polarization-media-habits>
- Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, 19(1), 54-61.
- Napier, J. L., & Jost, J. T. (2008). Why are conservatives happier than liberals?. *Psychological Science*, 19(6), 565-572.
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing*, 19(1), 27-41.
- Republican Platform 2020. (2020) from https://prod-cdn-static.gop.com/docs/Resolution_Platform_2020.pdf.
- Scharf, S. (2007). Report Casts Doubt on the Impact of Data Breaches on Identity Theft. *Internal Auditor*, 64 (4), 23.
- Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, 19(1), 62-73.
- Smith, H., Milberg, S., & Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2), 167-196.

Wojcik, S. P., Hovasapian, A., Graham, J., Motyl, M., & Ditto, P. H. (2015). Conservatives report, but liberals display, greater happiness. *Science*, 347(6227), 1243-1246

APPENDIX A: STUDY 1

RETAIL SITUATION

On the following screen, you'll be asked to consider a common shopping scenario. Please read the scenario carefully, imagining yourself as a shopper in this situation, and then answer the questions that follow.

National Retailer

Imagine you are visiting the website of a well-known national book retailer. The retailer offers special pricing and free shipping for customers that sign up for a membership. The membership requires you to enter your personal information including your full name, address, and credit card information.

Local Retailer

You are visiting the website of a local independent book retailer. The retailer offers special pricing and free shipping for customers that sign up for a membership. The membership requires you to enter your personal information including your full name, address, and credit card information.

Intention to Reveal Information (From MacKenzie and Spreng 1992)

Given this hypothetical scenario, specify the extent to which you would reveal your personal information through the Internet to this company.

	1 (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (7)	
Unlikely	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Likely
Not probable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Probable
Unwilling	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Willing

Trusting & Risk Beliefs (Adapted from Malhotra 2004)

Please indicate the extent to which you agree or disagree with the following statements.

	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
This company would be trustworthy in handling my personal information. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I trust that this company would keep my best interests in mind when dealing with my personal information. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Companies similar to this one are in general predictable and consistent regarding the usage of personal information. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

This company is always honest with customers when it comes to using the personal information I would provide. (4)

In general, it would be risky to give my personal information to this company. (5)

There would be a high potential for loss associated with giving my personal information to this firm. (6)

There would be too much uncertainty associated with giving my personal information to this firm. (7)

Providing
this firm
with my
personal
information
would
involve
many
unexpected
problems.
(8)

CONSUMER PRIVACY QUESTIONS

Please indicate the extent to which you agree or disagree with the following statements.

Control (From Malhotra 2004)

Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used and shared.

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)

Consumer control of personal information lies at the heart of consumer privacy.

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)

I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)

Awareness of Privacy Practices & Collection (Adapted from Smith et al 1996 for Internet)

Please indicate the extent to which you agree or disagree with the following statements.

	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
Companies seeking information online should disclose the way the data are collected, processed, and used. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A good consumer online privacy policy should have a clear and conspicuous disclosure. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is very important to me that I am aware and knowledgeable about how my personal information will be used. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It usually bothers me when online companies ask me for personal information. (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

When online companies ask me for personal information, I sometimes think twice before providing it. (5)

It bothers me to give personal information to so many online companies. (6)

I'm concerned that online companies are collecting too much personal information about me. (7)

Unauthorized Secondary Use (From Smith et al 1996 adapted for the Internet)

Please indicate the extent to which you agree or disagree with the following statements.

	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
<p>Online companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information. (1)</p>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<p>When people give personal information to an online company for some reason, the online company should never use the information for any other reason. (2)</p>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Online companies should never sell the personal information in their databases to other companies.
(3)

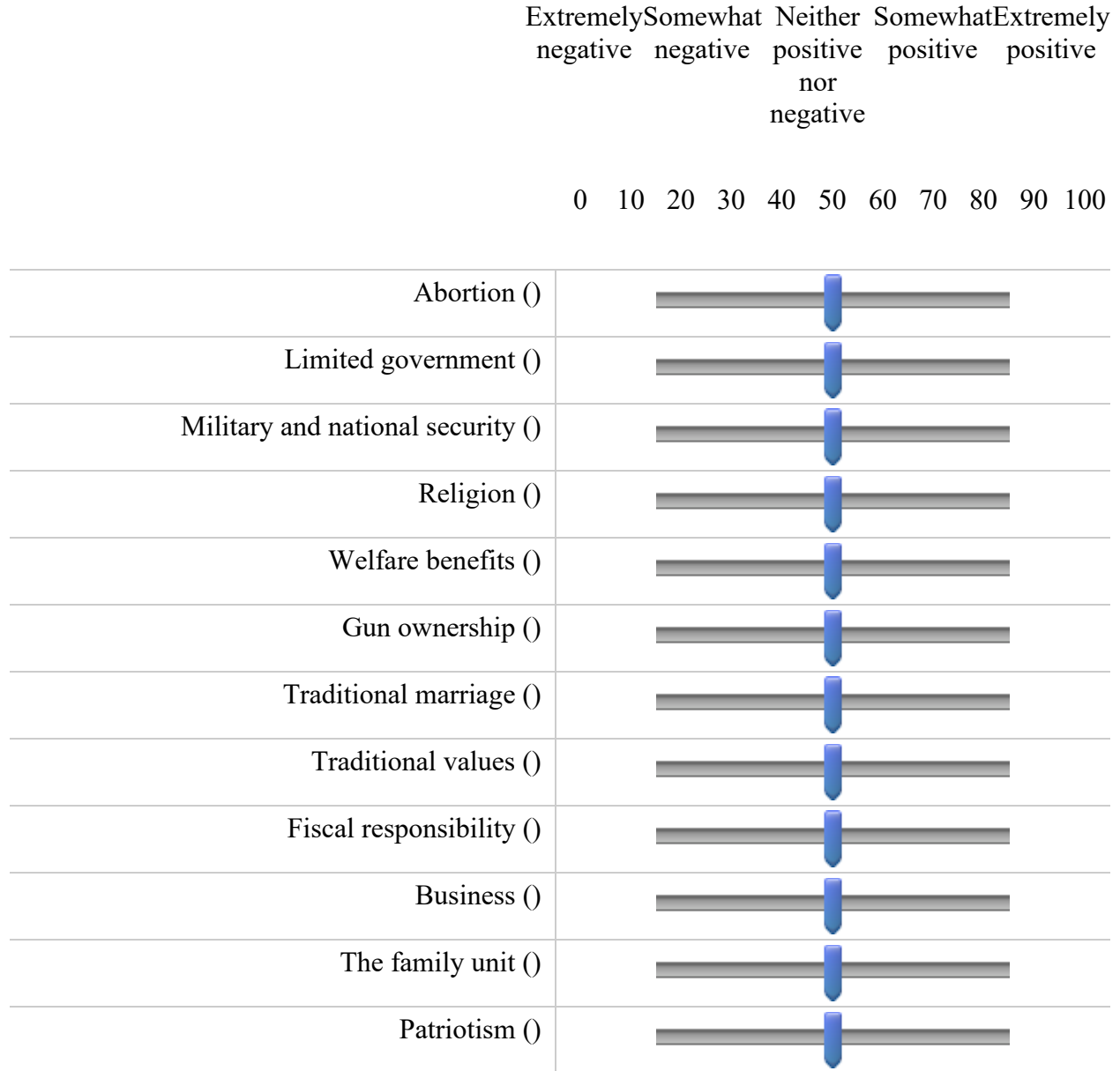


Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.
(4)



POLITICAL IDENTITY MEASURES (SECS, Everett 2013)

Please indicate the extent to which you feel positive or negative towards each issue. Scores of 0 indicate greater negativity, and scores of 100 indicate greater positivity. Scores of 50 indicate that you feel neutral about the issue.



ONLINE SHOPPING HABIT MEASURES

Some website ask for you to register with the site by providing personal information. When asked for such information, what percent of the time do you falsify the information? (From Malhotra 2004)

- I have never falsified information (1)
- Under 25% of the time (2)
- 26-50% of the time (3)
- 51-75% of the time (4)
- Over 75% of the time (5)

How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet?

- A great deal (1)
- A lot (2)
- A moderate amount (3)
- A little (4)
- None at all (5)

How often do you shop online?

- 0-1 times a week (1)
- 2-3 times a week (2)
- 4-5 times a week (3)
- More than 5 times a week (4)

How likely are you to make a purchase valued at over \$500 on the Internet?

- Extremely unlikely (1)
- Somewhat unlikely (2)
- Neither likely nor unlikely (3)
- Somewhat likely (4)
- Extremely likely (5)

To your knowledge, what is the most you have ever spent on one transaction on the Internet?
Please enter a number below.

How often do you save your personal information including credit card information and shipping address to your online shopping profiles?

- Never (1)
- Sometimes (2)
- About half the time (3)
- Most of the time (4)
- Always (5)

Have you ever signed up for a debit or credit card through a retailer?

Yes (1)

No (2)

If yes, how many different retailers do you have debit or credit cards through?

1-2 (1)

3-4 (2)

5 or more (3)

Not applicable (4)

DEMOGRAPHICS

Gender

- Male (1)
- Female (2)
- Non-binary / third gender (3)
- Prefer not to say (4)

Age

- 18 - 24 (1)
- 25 - 34 (2)
- 35 - 44 (3)
- 45 - 54 (4)
- 55 - 64 (5)
- 65 or older (6)

Education

- Some school, no degree (1)
- High school graduate (2)
- Some college, no degree (3)
- Bachelor's degree (4)
- Master's degree (5)
- Professional degree (6)
- Doctorate (7)

What political party do you identify with most?

- Constitution (1)
- Democrat (2)
- Green (3)
- Liberterian (4)
- Republican (5)
- Other (6)

Income level

- Less than \$10,000 (1)
- \$10,000 - \$19,999 (2)
- \$20,000 - \$29,999 (3)
- \$30,000 - \$39,999 (4)
- \$40,000 - \$49,999 (5)
- \$50,000 - \$59,999 (6)
- \$60,000 - \$69,999 (7)
- \$70,000 - \$79,999 (8)
- \$80,000 - \$89,999 (9)
- \$90,000 - \$99,999 (10)
- \$100,000 - \$149,999 (11)
- More than \$150,000 (12)

APPENDIX B: STUDY 2

RETAIL SITUATION

On the following screen, you'll be asked to consider a common shopping scenario. Please read the scenario carefully, imagining yourself as a shopper in this situation, and then answer the questions that follow.

National Retailer

Imagine you are visiting the website of a well-known national book retailer. The retailer offers special pricing and free shipping for customers that sign up for a membership. The membership requires you to enter your personal information including your full name, address, and credit card information.

After 6 months of enjoying your membership, the retailer experiences a data security breach. All of your personal information has now been compromised.

Local Retailer

You are visiting the website of a local independent book retailer. The retailer offers special pricing and free shipping for customers that sign up for a membership. The membership requires you to enter your personal information including your full name, address, and credit card information.

After 6 months of enjoying your membership, the retailer experiences a data security breach. All of your personal information has now been compromised.

Attitude Toward Retailer

Given the hypothetical scenario, please describe your attitude toward this company.

	1 (1)	2 (2)	3 (3)	4 (4)	5 (5)	
Dislike a great deal	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Like a great deal
Extremely negative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Extremely positive
Very dissatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Satisfied

Repatronage Intentions

Given this hypothetical scenario, specify the extent to which you would shop with this company again.

	1 (1)	2 (2)	3 (3)	4 (4)	5 (5)	
Unlikely	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Likely
Not probable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Probable

Improper Access (From Smith et al 1996 adapted for the Internet)

Please indicate the extent to which you agree or disagree with the following statements.

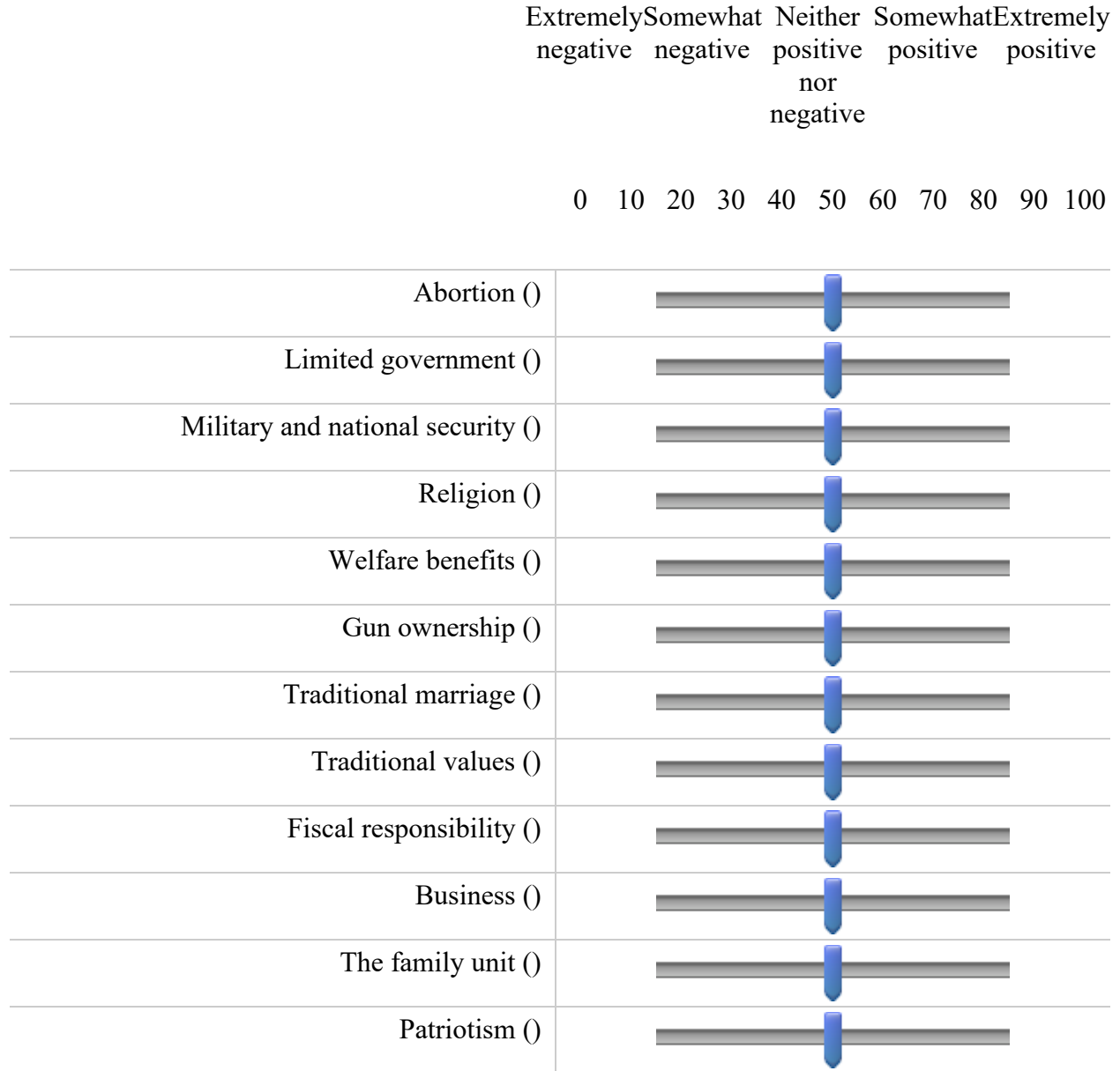
	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
This company should devote more time and effort to preventing unauthorized access to personal information. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This company should take more steps to make sure that unauthorized people cannot access personal information in their computers. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This company was unprepared for this data breach. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I would trust
this
company
with my
personal
information
in the future.
(4)

In general, it
would be
risky to give
my personal
information
to this
company
again. (5)

POLITICAL IDENTITY MEASURES (SECS, Everett 2013)

Please indicate the extent to which you feel positive or negative towards each issue. Scores of 0 indicate greater negativity, and scores of 100 indicate greater positivity. Scores of 50 indicate that you feel neutral about the issue.



ONLINE SHOPPING HABIT MEASURES

Some website ask for you to register with the site by providing personal information. When asked for such information, what percent of the time do you falsify the information? (From Malhotra 2004)

- I have never falsified information (1)
- Under 25% of the time (2)
- 26-50% of the time (3)
- 51-75% of the time (4)
- Over 75% of the time (5)

Please indicate the extent to which you relate with the following statement:
I falsify personal information on the Internet because I think it will be stolen.

	1 (1)	2 (2)	3 (3)	4 (4)	5 (5)	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree
Never true	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Always true
Does not describe my feelings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Clearly describes my feelings

How much have you heard or read during the last year about customers having their personal information stolen from the Internet?

- A great deal (1)
- A lot (2)
- A moderate amount (3)
- A little (4)
- None at all (5)

How often do you shop online?

- 0-1 times a week (1)
- 2-3 times a week (2)
- 4-5 times a week (3)
- More than 5 times a week (4)

How often do you save your personal information including credit card information and shipping address to your online shopping profiles?

- Never (1)
- Sometimes (2)
- About half the time (3)
- Most of the time (4)
- Always (5)

Have you ever signed up for a debit or credit card through a retailer?

Yes (1)

No (2)

If yes, how many different retailers do you have debit or credit cards through?

1-2 (1)

3-4 (2)

5 or more (3)

Not applicable (4)

Has your personal data information been part of a data breach from signing up from a credit or debit card through a retailer?

Yes (1)

No (2)

Not applicable (3)

If yes, have you continued to shop with that retailer?

Yes (1)

No (2)

Not applicable (3)

DEMOGRAPHICS

Gender

- Male (1)
- Female (2)
- Non-binary / third gender (3)
- Prefer not to say (4)

Age

- 18 - 24 (1)
- 25 - 34 (2)
- 35 - 44 (3)
- 45 - 54 (4)
- 55 - 64 (5)
- 65 or older (6)

Education

- Some school, no degree (1)
- High school graduate (2)
- Some college, no degree (3)
- Bachelor's degree (4)
- Master's degree (5)
- Professional degree (6)
- Doctorate (7)

What political party do you identify with most?

- Constitution (1)
- Democrat (2)
- Green (3)
- Liberterian (4)
- Republican (5)
- Other (6)

Income level

- Less than \$10,000 (1)
- \$10,000 - \$19,999 (2)
- \$20,000 - \$29,999 (3)
- \$30,000 - \$39,999 (4)
- \$40,000 - \$49,999 (5)
- \$50,000 - \$59,999 (6)
- \$60,000 - \$69,999 (7)
- \$70,000 - \$79,999 (8)
- \$80,000 - \$89,999 (9)
- \$90,000 - \$99,999 (10)
- \$100,000 - \$149,999 (11)
- More than \$150,000 (12)