RISKY BUSINESS: USING HEURISTIC-SYSTEMATIC PROCESSING THEORY TO UNDERSTAND CONSUMER DATA PRIVACY CONCERNS IN AN ONLINE BEHAVIORAL ADVERTISING CONTEXT

A Dissertation

presented to

the Faculty of the Graduate School

at the University of Missouri-Columbia

In Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

---

by

HEATHER SHOENBERGER

Dr. Esther Thorson, Dissertation Supervisor

DECEMBER 2014

The undersigned, appointed by the dean of the Graduate School, have examined the dissertation entitled

RISKY BUSINESS? USING HEURISTIC-SYSTEMATIC PROCESSING THEORY TO UNDERSTAND CONSUMER DATA PRIVACY CONCERNS IN AN ONLINE BEHAVIORAL ADVERTISING CONTEXT

presented by Heather Shoenberger,

a candidate for the degree of doctor of philosophy,

and hereby certify that, in their opinion, it is worthy of acceptance.

Professor Esther Thorson
Professor Peter Bloch
Professor Paul Bolls
Professor Glenn Leshner
Professor Shelly Rodgers

…….To Mom and Dad, the best people in the world. I would be a tiny, insignificant wallflower if I'd not grown up in your love and had you to lean on and learn from. I strive to be as kind hearted and brave as you both are.

ACKNOWLEDGEMENTS

I count myself among the most fortunate for getting the chance to study at the University of Missouri School of Journalism; an experience that was nothing short of magical. I've grown into a better and more capable person. It was not the program but the inspirational and kind professors who inhabit the school that made this experience possible. I would most especially like to thank Dr. Esther Thorson who supported me from the minute I walked into her office. Her enthusiasm and endless energy are contagious. I would not be where I am without her guidance and support. Thank you is also due to Dr. Paul Bolls, a friend with whom a conversation about practicalities could easily end up down the rabbit hole of ideas. Thank you to Dr. Glenn Leshner who showed me how to calmly instruct methods courses and always has a moment to discuss research or life. Thank you to Dr. Shelly Rodgers whose methodical approach to research has and will continue to help me in my career. Dr. Peter Bloch, thank you for your support during my time at Mizzou.

I would also like to thank Professor James Devine. While you passed on just before I began at the J-School in 2010, I am thankful you pushed me to get a PhD and for your advice. Thank you also to Professor Wes Pippert for suggesting that a PhD may be the best route for me.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

Despite the possibility for misuse of their data, and previous research expressing consumer concern over privacy consumers continue to shop online. This study tests the idea that consumers' navigation online leading to eventual purchases online is so ritualized and driven by short-cuts (e.g., brand familiarity) that processing information about the privacy safety offered by individual websites is mostly under the control of heuristic information processing. This study hopes to offer an explanation for the privacy paradox (despite apparent privacy concerns, Internet users rarely take self-protective measures to alleviate those concerns) and additionally, privacy concerns online seem to have little effect on consumer behavior when on the Internet. Implications for regulators and advertising practitioners into the complex processes involved in consumer privacy concerns and online data collection.

I. INTRODUCTION

Supreme Court Justices Samuel Warren and Louis Brandeis noted in an 1890 Harvard law review that new technologies could cause what was once whispered behind closed doors to one day be screamed from rooftops (Warren and Brandeis 1890). Though originally conceived as a worry focused on governmental violation of consumer privacy, the justices' concerns about surveillance of consumers' information and privacy issues foreshadow those of consumer advocates as advertisers and online retailers continue to amass consumer data in an effort to serve more relevant content to their consumers. Platforms such as Facebook pages and Google searches may have replaced the "rooftops" but the issue of consumer privacy has grown increasingly important and is being discussed at length by the current administration, the FTC, consumer advocates, and the advertising industry. For example, a recent White House report included a note in its recommendations for protecting consumer privacy in the online based economy that "many consumers and privacy advocates find tracking and the advertising practices that it enables invade their expectations of privacy" ("Consumer Data Privacy In a Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Digital Global Economy" 2012). Consumer privacy concerns arise every time a person clicks from site to site and when they make purchases. Some research has pointed to the lack of knowledge consumers have about the way data is collected online which in turn leads them to distrust advertising that results from such collection (McDonald 2010). Additionally, previous reports have noted that such data collection could lead to changes in consumer behavior online such as a change in purchase intentions after learning about

how data is collected (Milne 2009) and used online, and that such collection could be perceived as invasive by the consumer (McDonald 2010).

Despite the possibility for misuse of their data, consumers continue to shop online. In the United States, e-commerce increases about 10% each year (Weinstein 2013). Additionally, consumers routinely express desire for privacy policies yet show little interest in paying attention to such policies, rarely taking proactive actions to protect their data (Joinson 2010; Metzger 2007). This lack of interest or notice of policies and the continued desire for policy as verbalized by consumers has led to what some call the "privacy paradox" (La Rose 2004; Yap, Beverland and Bove 2009; Norberg, Horne and Horne 2007).

Ecommerce shows no signs of slowing, online behavioral advertising spending online is projected to increase (eMarketer 2013) and the voluminous amounts of data collected and stored to serve relevant advertisements opens the door for a plethora of data privacy and security issues. Advertisers use clickstream data and data entered into websites to serve advertisements relevant to a consumer's online behavior, a type of consumer targeting that allows consumers to receive information about products and services that they may be interested in, (eMarketer 2013) and allows advertisers and marketers to more efficiently communicate to their audiences. Advertisers are able to pay companies to use tracking technologies to create profiles of users based on clickstream data and then offer advertisements based on that profile ("Online Tracking and Behavioral Profiling" 2014). However, the practice of online behavioral advertising (OBA) is riddled with controversy as consumers and advertisers negotiate the balance between privacy concerns and information flow.

The importance of this study is paramount to uncover both ways in which consumers navigate the online economy (in the narrow context of online search and shopping data collected on websites and aggregated by third parties to produce relevant advertisements), to offer an explanation for the privacy paradox, and offer insight for regulators and advertising practitioners into the complex processes involved in consumer privacy concerns and online data collection.

The privacy issue stems from the assumption that the information collected and aggregated is, in some ways, regarded by the consumer as information that should not be shared without explicit permission and that the consumer should have a measure of control over how it is used. The method of regulation by the Federal Trade Commission and adopted by many advertisers as a self-regulation policy is that of allowing the consumer the ability to opt-out of activities online that may result in their data being used by other entities. The idea behind any kind of opt-in or opt-out system is to allow consumers control over information they provide about themselves. Because privacy is a socially constructed term (Solove 2006), it is often operationalized by regulators as a more tangible concept of control and when consumers ignore privacy policies or information that may allow control over that data, the issue becomes more contentious (Joinson 2010; Metzger 2007).

The issue of privacy in the realm of data collection online continues to appear in the news and ignite debates among consumer advocates and regulators alike (Podesta, Pritzker, Moniz, Holdren, and Zients 2014; Sableman, Shoenberger and Thorson 2013; Consumer Data Privacy In a Networked World: A Framework For Protecting Privacy And Promoting Innovation In the Digital Global Economy 2012; McDonald and Cranor

2010; Turow et. al. 2009). Yet, news coverage alone, even a series entitled "What They Know" run by the *Wall Street Journal* ("What They Know" 2010-2012), has not been enough to encourage consumers to pay attention to privacy policies let alone opt-out of tracking of clickstream data online (Sanger and Lohr 2014**)** despite studies noting that media may have influenced behavior in this realm (Poddar, Mosteller, Ellen 2009)**.** In fact, though studies allude to the idea that consumers desire more privacy protections online (McDonald and Cranor 2010; Turow et. al. 2009) according to a recent White House report, consumers almost always click on terms of agreement without reading them, adding incentive for privacy advocates and researchers to wonder whether the opt-out system and current privacy policies are effective at ensuring consumers have adequate control over their data (Sanger and Lohr 2014; Leon, Ur, Shay, Wang, Balebako and Cranor 2012). This issue may be more pronounced in the area of clickstream data collection and the use of such data to serve relevant advertising (online behavioral advertising or "OBA") as people are not asked to click on an agreement at all but instead may opt-out of click stream data collection, if they are aware of the process or desire to do so. This type of data collection is examined in this study.

The issue of advertiser collection and use of consumer data online has been examined from the assumption that the consumer is actively able and willing to search for information to protect her privacy and make decisions about when to disclose information to a website based on a rational, thoughtful process (Poddar, Mosteller, Ellen 2009; Milne, Labrecque, and Cromer 2009; McDonald and Cranor 2010; Turow et al 2009). This body of research has also largely focused on consumer disclosure of personal information to a website (see Norberg, Horne and Horne 2007 for a study largely based

on heuristic theory but dealing with disclosure of information to websites). Online behavioral advertising does not necessarily demand online disclosure in the form of filling out information. An item added to a cart, even if not purchased or clicking through a brand's website may lead to an advertisement of that item(s) to follow the consumer to another site. The information is not personally identifiable but is aggregated in large databases in an effort to better serve relevant advertising based on profiles created with online clickstream and surfing behavior. The world today is complex and saturated with information. Theoretically, it is possible that people are using heuristics to guide their behaviors online as they do in so many other facets of life (Chaiken 1980; Gigerenzer and Gaissmaier 2011; Gigerenzer 2009).

This study uses Shelly Chaiken's Heuristic-Systematic Processing Model as a lens through which to help explain how consumers navigate the online economy to examine an explanation for the privacy paradox (Chaiken 1980). It examines the issue of consumer behavior online and the voiced desires for additional regulation and privacy concerns from the theoretical standpoint that most consumer behavior online is driven by heuristics which are strategies employed by humans to make faster decisions, conserving mental energy and ignoring some information than a more systematic and well-reasoned approach (Gigerenzer and Gaissmaier 2011; Chaiken 1980).

What is tested here is the idea that consumers' navigation online leading to eventual purchases online is so ritualized and driven by short-cuts (e.g., brand familiarity) that processing information about the privacy safety offered by individual websites is mostly under the control of heuristic information processing (Siegrist 2000; Chaiken 1980). That is, people use existing knowledge structures or cues like brand familiarity to

determine whether to go to and interact with websites rather than systematically checking information about the sites before they venture through them. It is theorized that in the online economy one of the most important heuristic cues is brand familiarity, presumably associated with extensive experience with the brand. For example, a person who surfs the site and/or shops at Jcrew.com several times a month is probably unlikely to stop and look at the company's website privacy policy, largely due to the overall familiarity and resulting trust in the brand itself that spills over to the site's safety and data handling procedures. However, a site that a consumer has never heard of or visited may present enough novelty and thus, perception of risk to warrant seeking information about the site privacy policy and additional information.

This study involves using scenarios people may encounter in real life while shopping online. The study also, unlike real life, alerts people in random fashion after a moment of calculation based on answers they provided previously that going to a website can trigger their clickstream data to be accumulated and used in ways they may disapprove of, or could embarrass them in some way. It is posited that people who are alerted to the risk of their online data being used in the aforementioned ways will be more likely to check the privacy policy of websites before they click through or purchase from them, something that currently is rarely, if ever done (Smit, Van Noort, and Voorveld 2014, Rifon, LaRose, Choi 2005). Additionally, it is posited that the high risk (low risk) condition will interact with brand familiarity, such that high brand familiarity will lessen the likelihood of a consumer seeking of additional information about a website before clicking through it or offering the information necessary for a purchase, while low brand familiarity will not. That the online economy operates in a vacuum is an assumption not

made here and thus, individual difference variables of interpersonal trust and institutional trust are examined as two other types of heuristics that are likely to be more socially driven

The individual difference variables of interpersonal trust and institutional trust may also play a role in how people perceive their risk online and desire for additional regulation despite the risk condition to which they are randomly assigned. Institutional trust and interpersonal trust are added as measured individual difference variables that enhance the context in which online behavioral advertising operates. With participation in e-commerce continuing to increase and advertising dollars increasingly being spent on messages made relevant through the use of clickstream data collected by cookies and other tracking technologies, it makes sense that there is some level of trust in one another and the institutions administering such advertising and those charged with policing e-commerce activities, even if that trust is misplaced.

This issue is of particular importance not only to advertisers looking to more efficiently communicate with their audience and consumer advocates concerned about the potential for personal data abuse but to regulators such as the Federal Trade Commission who assume a conscious, economical processing of safety online, conceptualizing privacy, in part as the ability to control one's data. The idea of control over one's data as a component of privacy requires a conscious effort on the part of the consumer to wield control over that data through decision-making that weighs the pros and cons involved. When a consumer relies on short-cuts (e.g., previous knowledge/experience with a brand or site and the resulting trust that a site will not do anything with their data that they are not aware of) a systematic evaluation of risks and benefits is not made and it is hard to

see the use of heuristics offering an economic argument made by the consumer about data control. Additionally, there may be error in the judgment made by the consumer using heuristics. In fact, heuristic processing may inflate error by either accepting that the site is safe when it isn't based on the reliance on mental short cuts or rejecting a site the consumer erroneously judges as unsafe (Chaiken 1980). If the consumer does not take the time to read and understand the use of online behavioral data on a website, the privacy policy and the suggestion by the FTC that consumers be given notice of how to control their data in online behavioral data collection processes may be seen as useless, though recent research into human reliance on heuristics has noted that the accuracy versus mental effort trade-off may not be as large a chasm as once believed as many heuristic cues are both usually accurate and time saving as far as mental effort (Gigerenzer and Gaissmaier 2011).

For the purposes of this study, the online economy is defined as the environment in which a consumer both shops on the Internet and casually browses the Internet, often putting items in their virtual shopping carts at businesses' sites only to see ads for items like the ones recently purchased or put in virtual shopping carts pop-up on websites like Facebook.com or other websites not affiliated with the initial site of interest. These "third-party" advertisements made relevant to a consumer based on online behavior are made possible by "cookies" or small text files placed on a computer by a "third-party" to collect and aggregate information on the online surfing behavior of the consumer ("Tracking Cookie" 2014).

There are a myriad of reasons a consumer discloses information online and/or does not opt-out of cooking tracking. These sorts of transactions result in a tradeoff

between the consumer and marketer or advertiser: one gets information to target information more efficiently and perhaps more economically, and the consumer may get cheaper/free content and/or more relevant information from marketers. This study specifically looks at the situation when consumers' clickstream data (online surfing behavior) and information offered to a website in order to make a purchase is aggregated by individual companies and big data aggregators to serve more relevant advertising.

Specifically this study seeks to answer the following questions: Whether alerting consumers to a personal risk involving their online behavioral data will motivate them to systematically process the brand site, by measuring symptoms of careful processing such as information seeking in an effort to glean sufficient information on how their data is used and protected on that site.

This study adds to the literature by first examining the idea that consumers are more reliant on heuristics to guide their behavior online with regards to privacy and security of their clickstream data than they are on systematically making rational, economical choices about when to disclose information online and what sites to trust. The phenomenon being studied here is perhaps the least transparent to the consumer. That is, when advertisers not only use actual shopping transactions where information is typed in and exchanged but data is aggregated about consumer behavior online without the solicitation of information, relying solely on cookies to record clickstream data and later aggregating that data alone or with purchase information to offer advertisements relevant to the search and online shopping behavior. Additionally, the variable of institutional trust is included as predictor over and above the risk manipulation in an effort to address

the complex context in which online behavioral data collection occurs in everyday life and the significance of institutional trust in the area of everyday safety concerns.

Additionally, suggestions will be made for what kind of regulations are necessary to maintain a balance between consumer privacy interests and the advertiser/marketers rights to disseminate information and the consumer's right to receive information (*Virginia State Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U.S. 748 (1976)).

2. LITERATURE REVIEW

Advertising professionals believe online behavioral advertising is integral to both the industry and consumers because it can offer relevant and thus, more positively received messages (Nyilasy & Reid, 2009a). To add leverage to this sentiment, digital advertising spending is expected to make up a quarter of all advertising spending around the world in 2014 (E-marketer.com 2014).

The increase in ad spending in the area of online behavioral ads comes on the heels of consumer preference for relevant to irrelevant advertising as suggested by several advertising studies that have shown that personal relevance has both direct and indirect effects on attitude to the ad. High levels of personal relevance have been shown to increase positive attitude while the opposite has been found true of low levels of personal relevance (Liberman & Chaiken, 1996). Further study by Claypool and colleagues (2004) found that participants shown relevant messages had increased positive disposition to the message as each message was repeated, however, attitude toward the repeated messages decreased when participants who received messages that were not personally relevant (Claypool, Mackie, Garcia-Marques, McIntosh and Udall 2004). The result of this body of research was a consensus that consumers preferred personally relevant messages to those that were not personally relevant (Campbell and Wright 2008).

Yet, some studies have reported consumers do not want tailored advertising and that OBA violates consumer privacy expectations and thus, in many cases, should be curtailed or have strict regulation applied (McDonald and Cranor 2010; Turow, King, Hoofnagle, Bleakley, and Hennessy 2009). Interestingly, Joseph Turow, one author from

the aforementioned studies, recanted his original perceptions of his own research and said, "Who in his right mind wouldn't want relevant ads over irrelevant ads (Goel 2014)." The admission does not change the fact that there is still a lack of understanding as to just how consumers negotiate the online economy. A gap exists in the literature on the examination of how consumers navigate the online economy, and the attempt to discover when consumer privacy interests emerge in the form of systematic or careful processing of information about consumer data in relationship to that economy.

When asked about their concerns online, consumers voicing concerns about privacy online seem to be approaching the privacy concept with conscious systematic processing or at the very least a socially constructed bias whereby the "right" response is always the response thought acceptable by society (Haidt 2012). In this case, the acceptable response includes indicating that additional privacy measures should be implemented and a consumer should indicate concern about their privacy. However, when consumers are not asked about their privacy or exposed to a message about the potential risks, it appears those shopping/surfing online seem to be doing so using "shortcuts" such as brand familiarity to guide their navigation online (Shoenberger and Thorson 2013). Though consumers routinely express desire for privacy policies, they show little interest in paying attention to such policies, rarely taking proactive actions to protect their data (Joinson 2010; Metzger 2007). This lack of interest or notice of policies and the continued desire for policy as verbalized by consumers has led to what some call the "privacy paradox" (La Rose 2004; Norberg, Horne and Horne 2007). Norberg and colleagues verified the existence of the paradox in an online information disclosure setting, noting in their discussion that now the task was to flesh out the antecedent conditions that may help

explain why the paradox exists (2007). The "privacy paradox" though noted by several researchers, has been rarely empirically examined (Yap, Beverland and Bove 2009) and, as discussed by Norberg and colleagues, is not yet fully understood.

In line with the privacy paradox phenomenon, research has suggested that even though consumers assert concern over their data privacy, there is little correlation between that concern and self-protective behavior (Regan 1995; Sheehan and Hoy 1999; Norberg, Horne and Horne 2007). Research implies that it is often the case that shopping, in general, is accomplished through the use of shortcuts such as using brand familiarity or habit to make decisions about the desirability of a product (DelVecchio 2005). In the literature, shortcuts are often referred to as heuristics (Chaiken 1980). Heuristics are "cues" used to guide behavior and are defined as "any variable whose judgmental impact is hypothesized to be mediated by a simple decision rule" (Chaiken, Liberman, and Eagly 1999, p. 216). For example, a familiar brand is likely to equate to perceptions of a safe brand website (recent breaches or low brand trust notwithstanding).

People who shop online know there are dangers from technology they do not understand (Rohm and Milne 1998; Miyazaki and Fernandez 2001), and they know there are frightening stories about what happens when people's private affairs are shared publicly (privacyassociation.org) but it doesn't seem to affect their shopping/surfing habits, perhaps because they have not been personally affected or threatened by potential data misuse, or because they are relying on trust in familiar brands and in a larger social context, institutional trust or trusting that the government, advertising industry, etc is going to keep them safe. It is likely that despite voiced concerns about data when asked on a survey, consumers continue to share online behavioral data and/or fail to opt-out,

especially in online business because they rely on "cues," that is, they rely on heuristics such as the trust they have in a brand to guide online behavior and it is only when they are asked about or alerted to immediate and personally relevant risks associated with data collection that they deem privacy to be a motivationally relevant issue to explore. The following literature review will first examine the relevant literature on the Heuristic-Systematic Processing Model as it applies to the issue of consumer concerns about privacy in the online economy and its ability to posit a plausible explanation for the privacy paradox. Then it will assess the relevant risk perception literature, and the literature speaking to brand familiarity as a heuristic and the individual variables of institutional trust and interpersonal trust within light of data collected for the purposes of online behavioral advertising. Lastly, to add context to this study in the political realm a portion of the Literature Review will be dedicated to online advertising context, and the concept of privacy in the online advertising context.

Heuristic-Systematic Processing Model

The idea that some cognitive processing is automatic is an old assumption (Uleman and Bargh 1989) but the assumption that most of the time, human beings possessed controlled, intentional and rational thought and decision making processes was the primary theory gripped cognitive psychology until the middle of the 1970s when the assumption of the rational decision maker was revisited (Uleman and Bargh 1989). By the late 1970s, some researchers had begun to reject the assumption that humans made most of their decisions through deliberate thought processes and the study of automatic thought, along with the reliance on heuristics in decision-making made a resurgence (Uleman and Bargh 1989).

Every day human beings rely on heuristics, or cues to guide their behavior. Starting at the physiological level, a person has no control over preconscious automaticity (Bargh 1989). This kind of activity has been likened to a reflex whereby they are triggered automatically by a certain stimulus with no conscious control asserted by the person. For example, in the instance of vision, there is an allocation of spatial attention to record the environmental stimuli, although the resources used in garnering that attention do not reach a conscious level, though are not thought to be entirely effortless (Bargh 1989). This idea makes sense as people must constantly scan their environments for elements of danger but cannot devote a great deal of effort in doing so or they would get nothing else done. Heuristics are rules of thumb that do not look to maximize the likelihood that they will lead to a predicted outcome as in the case of statistics but instead are considered to be frugal or looking to satisfice (Gigerenzer 2008). Heuristics fill the brain with tools to be used to adapt to certain situations and allow people to do so with minimal cognitive effort (Gigerenzer 2008). Heuristic processing is often thought of as less useful or error prone in contrast to more systematic or effortful processing of a stimuli or situation. However, Gigerenzer (2008) notes that this is not the case, that not only are heuristics used in an adaptive way when cognitive resources are limited but also when the problem presented may not be able to be solved through a more rational process. One example would be selecting a friend (not able to be rationally thought out with an optimal solution reached) versus playing a game like tic-tac-toe (Gigerenzer 2008). Additionally, heuristic cues can be arranged to allow human beings to rely on the most important heuristics within a certain situation to adapt to a complex environment where some of the

information has to be ignored (Gigerenzer 2008). In the present study, heuristics will be examined as useful cues that guide consumer behavior online.

The Heuristic-Systematic processing model asserts that individuals will use either or both the heuristic or systematic processing systems in an effort to evaluate information and come to a conclusion (Trumbo 1999). The theory assumes that systematic processing happens when an individual exerts "considerable cognitive effort" and "actively attempts to comprehend and evaluate the message's arguments as well as to assess their validity in relation to the message's conclusion" (Chaiken, 1980, p. 752). On the other hand, heuristic processing occurs when the emphasis is not on conscious effort but on the "role of simple rules or cognitive heuristics" which are formed by previous information that the individual has stored conceptually as knowledge structures (p. 752). Heuristic processing is not conceptualized as effortless processing, though at times it may share criteria for the concept of "automaticity" or lack of conscious awareness (Chaiken, Liberman and Eagly 1989). Other times, individuals actively search for heuristic cues to guide their judgments (Chaiken, Liberman and Eagly 1989). The most important distinction is that systematic processing is theorized to take significantly more cognitive effort and inspection of a message than heuristic processing. Heuristic processing has been identified in studies like the one where a message is kept constant and the manipulation is the likeability of the speaker. Holding the message constant, the more liked speaker led to indications of a more liked speech (Chaiken 1986).This heuristic was deemed the liking-agreement heuristic or the assumption that people usually agree with people they like (Chaiken, Liberman and Eagly 1989). Another example is found with brand familiarity as a heuristic. Another study found that people generally preferred high

quality peanut butter. However, when a familiar brand label was placed on a low quality peanut butter jar, the participants indicated a preference for the branded peanut butter (Hoyer and Brown 1990). Both studies illustrated a heuristic cue at work.

Heuristic processing tends to be the rule for most information processing due to the need for an both appropriate amount of cognitive resources and the motivation to systematically process a message (Maheswaran, Mackie, and Chaiken 1992). Put simply, humans are constantly looking to minimize the amount of cognitive effort expended. Simple rules or short-cuts are used to reduce the cognitive effort and are used to judge the environment because they have proved reliable in the past (Averback, Jones and Robertson 2011). When an individual has only a small amount of prior information, there is not likely to be an attitude developed that is relevant to the topic of the message. Thus, being able to use a heuristic, or a previous piece of knowledge to arrive at a conclusion based on a cue or short-cut, is important for the individual (Averberck, Jones and Robertson 2011).

Though, heuristic processing is considered the most common of the dual processing model the two processes can co-occur (Griffin, Dunwoody, Nuewirth 1999, Chaiken, Liberman and Eagly 1989). Heuristic cues are assumed to be less persuasive when the individual is able and motivated to examine information systematically and in the contrast, more persuasive (assuming their existence in the information presented) when the individual has less cognitive ability available and limited motivation to process systematically (Chaiken, Liberman and Eagly 1989. Most of the research in this area has been in an experimental setting starting with the seminal Chaiken study published in 1980, but some research is also being conducted via survey methods as HSM is applied to

other contexts such as risk communication (Kahlor, Dunwoody, Griffin, Neuwirth, and Giese 2003).

Although the Heuristic-Systematic Processing Model was developed to address persuasion contexts, Chaiken encouraged its expansion to other contexts (Chaiken, Libeman and Eagly 1989). For instance, the theory can be applied as a framework for a large range of environments where a person's decision making process is the focus. The idea that the use of heuristic cues may be the driver of consumer behavior in the context of online data collection, disclosure and shopping was derived from what is referred to as the game of give and take which is attributed by evolutionary psychologists as a necessary but sometimes flawed mechanism behind human behavior and survival (Simmel 1978, Luhmann 1979). The idea is that humans, in an effort to lead more efficient lives, began to make pre-commitments or giving something of value to another with the expectation that the other will, in the future, return with something of value. Inherent in the game of give and take is risk but also, the foundation of trust (Nooteboom 1975). According to evolutionary psychologists, humans are hard-wired to partake in the game of give and take in an effort to lead productive and efficient lives and thus, perhaps hardwired to use heuristics to guide daily decision making (Nooteboom 1975). The online economy would be less efficient if every transaction warranted cognitive effort and a conscious weighing of risks and benefits. Additionally, the convenience of online shopping and relative enjoyment of surfing online may diminish if the consumer had to constantly put forth effortful concentration and expend cognitive resources to the risk/benefit analysis before clicking to the next site.

An individual may be more likely to carefully evaluate the safety of their data on a particular website if they are motivated to do so. Because the Heuristic-Systematic Processing Model is based on effort and capacity assumptions and heuristic processing in the rule instead of the exception, an individual requires motivation to systematically process but also the cognitive resources to do so. Motivation as the driver of systematic processing when there is the cognitive ability to do so has been supported by voluminous literature (see Chaiken 1987; Chaiken and Stangor 1987; Petty and Caccioppo 1986 and Chaiken, Liberman and Eagly 1989). Motivations were manipulated in these studies by exposing individuals to messages with high (low) personal relevance, who were led to believe that their judgment had important consequences. Those in the high motivated conditions exerted more effort/systematically processing as measured by time spent reading the message, recall of arguments, more elaboration through thought listing (Chaiken, Liberman and Eagly 1989). While the systems can be employed simultaneously, a heuristic judgment is made using a cue such as brand familiarity while a systematic judgment would be one arrived at upon tasting and deliberating each jar of peanut butter as mentioned in the above example. Those individuals under time constraints or other impairments to cognitive capacity were less likely to systematically process even with heightened motivation to do so (Chaiken, Liberman and Eagly 1989).

Essentially, heuristics allow for efficiency in everyday life but may come at a price, though recent research discusses the possibility that the costs are minimal (Gigerenzer 2008). There is error that may come into play when someone relies on a short-cut to make a judgment (Chaiken 1980). For example, a person may rely on a short-cut that a brand is trustworthy based on previous experience but later find out that it

was selling their data to third parties, something they disapproved of. However, the individual is likely to carefully evaluate their environment when a risk is introduced (Turner, Mitchell and Rimal 2006) increasing risk perception and as a result, information seeking and systematic processing. For example, the individual may be more likely to carefully evaluate the privacy information on a website (e.g., privacy policy) if alerted to the risk of their data being stolen online. Otherwise, the individual may use simple cues such as the attractiveness of a spokesperson to arrive at a conclusion about the message the spokesperson delivers with no emphasis on the content of the message. For example, if a celebrity endorses a washing machine in an advertisement, the advertisement may be effective for the person who is looking to purchase a washing machine but likes the celebrity whereas someone in the market for a new washing machine may be less affected by the celebrity and systematically process the contents of the message (Averbeck, Jones and Robertson 2011).

Once a risk or incongruency in information is introduced and systematic processing is at work, the sufficiency principle applies. The principle asserts that an individual will exert the effort necessary to attain confidence in their judgment of content. Thus, when there is no prior knowledge structure with which to use heuristics or when the use of heuristics does not supply the information necessary to feel confident in one's judgment, systematic processing will occur (Chaiken, Liberman and Eagly 1989). The motivation of personal relevance, manipulated in this study with personally relevant information about the risk of an individual's online data, is assumed to influence the effort given to processing because it affects the individual's sufficiency threshold. In other words, when content becomes personally relevant, the individual is theorized to

desire more information about the content in an effort to reach a higher level of confidence in their attitude and/or judgment about the content (Chaiken, Liberman and Eagly 1989). Thus, if they perceive a personal risk to their data online, they will be motivated to search for additional information about mitigating that risk.

Based on findings of previous studies conducted on the issue of online behavioral data collection, it seems that the consumers' voiced privacy concerns online are triggered by rational, systematic processing but that effortful, systematic processing is not happening when consumers are surfing online in a real-life or natural setting due to the lack of self-protective behaviors exhibited and the continued growth of e-commerce despite the voiced concerns (Sableman et. al. 2013; Shoenberger and Thorson 2014). It would seem that if the consumer was consciously weighing privacy concerns in a conscious and effortful way, she would actively seek out information about how the data collection worked and what it was used for but that doesn't seem to happen as noted in previous research belying consumers' poor sense of how online data collection works or why it is used (Smit et. al. 2014; Shoenberger and Thorson 2014). The idea that knowledge is a poor predictor of privacy concerns online may seem counterintuitive but is a common finding in the area of complex sciences and new technologies (Brossard, Scheufele, Kim and Lewenstein 2009). As Chaiken notes, motivations that lead to systematic processing are contextual and driven also by individual factors (Chaiken, Liberman and Eagly 1989). It appears that in this context, knowledge of the complexities of the technology of online tracking and resulting targeted advertising are not motivations capable of producing systematic processing in the context of the online economy,

specifically in the context of online tracking and the relevant advertising served to consumers as a result of an online profiled compiled by that tracking.

It is theorized that for most data exchanges online the consumer is relying on the short-cuts or heuristics to navigate the online economy unless motivated to systematically process. The consumer may be more apt to carefully, systematically process the information if a personal risk is made salient.

Risk Perception as Motivation

The Risk Information Seeking Perception Model has worked to identify the important factors that lead an individual to search for additional information and systematically process information (Griffin, Dunwoody, and Neuwirth 1999). The model was constructed, in part, based on the premise of the Heurisitic Systematic Model (HSM) (Yang, Aloe, and Feeley 2014) and works well within its parameters. The model posits, like the HSM, that individuals who process information systematically, carefully do so because they lack information sufficiency (Yang et. al. 2014). For example, if an individual is exposed to a personally relevant risk they may be more likely to want to know what is happening with their online data and may click to find out what the policy is because they perceive risk to their data in the online environment. Increasing their knowledge, or information seeking may remedy that once they have reached a sufficient amount of information necessary to satisfy their processing aims (Eagly and Chaiken 1993; Yang et. al. 2014). Personally relevant information has predicted information seeking behavior in circumstances of perceived risk (Ter Huume and Guttelng 2008). Based on the literature, it seems to follow that risks that are perceived as personally

relevant, such as a compromise of consumer data, are likely to elicit information seeking behavior (Ter Huume and Guttenlng 2008).

High perceived risk with low/moderate fear may translate to systematic processing through motivation to seek additional information in the content and not just cues, such as privacy policies of a brand's advertisement as a protective measure (Turner, Rimal and Morrison 2006). Previous research has found perceived risk to occur through cognitive evaluation which would implicate systematic processing (Dholakia 2001). In the consumer psychology literature, perceived risk has been theorized to present itself when there is an unanticipated and uncertain set of consequences resulting from buying a product (Bauer 1960). One distinction the consumer psychology literature makes about risk perception in comparison to other branches of psychology is that risk perception is thought to arise only through the possibility of negative events and not a risk/benefit calculation (Dholakia 2001) and has been defined as perceived potential for personal harm (Ter Huurne and Gutteling 2008).

From the health communication literature, the Risk Perception Attitude Framework posits that when risk perception and perceived efficacy are high people are likely to seek out information about the risk (Turner et al 2009). Even those with high perceived risk and low efficacy tend to information seek, though their retention of the information sought is significantly lower than those with high perceived risk and high efficacy, a phenomenon thought to be linked, perhaps, to the anxiety reduction hypothesis (Turner et. al 2009). However, in the realm of health risk communication, more fearful people were more likely to defensively process health risk information while those with low to

moderate fear did not appear to be on the defensive and processed in the health risk information in a careful, and objective way (Biek, Wood and Chaiken 1996).

The perception of risk in the online economy can be abstract for consumers who may not be able to visualize the threats of data misuse they may be subject to in contrast to a more tangible risk of contracting an illness. Because this study is interested in when consumers are motivated to systematically process and search for information about the risks they may encounter in the online economy, only the high risk and high efficacy condition is of theoretical importance.

Consumer online data privacy breaches are not risks associated with physical pain or ailments, but consumer data collected online and attached either by inference or through personally identifiable links could cause embarrassment, anxiety, job loss, the loss of a job, denial of certain benefits or discrimination (Podesta et. al. 2014). The risks associated with loss of control over ones data has been coined a diffused risk (Turrow and Hennessey 2007) and as a result, may not motivate attention to privacy as a more salient risk might.

We theorize that if alerted to the potential misuse of data and the embarrassing and dangerous consequences associated with that misuse, consumers will be more likely to seek out information about how their data is being used to serve a certain type of advertisement. Higher perceived risk has consistently been linked to information search as a way to reduce risk (Dholkia 2001; Richens and Root-Schaffer 1998; Neuwirth, Dunwoody, and Griffin 2000). However, a necessary condition to motivate information search behavior is situational involvement (Dholkia 2001). Thus, the risk must be considered personally relevant to the consumer to elicit information seeking behavior.

The present study seeks to induce the desire for information in times of perceived personal risk by manipulating risk perception. It is theorized that people in the high risk group will systematically process website information by reporting a desire for additional information about how their data is used and other information about the site and perceive greater privacy risk, and less control over their data.

The types of risk involved in this study involve consumer data being used in ways that consumers have not previously approved of and represents a loss of control over the data. Heuristic cues are likely to mitigate any feelings of risk even in the face of the risk manipulation, especially in the scenarios, brand familiarity.

Brand Familiarity as a Heuristic in the Online Economy

As noted earlier, a heuristic is any variable that mediates a consumer's attitude or judgment about a particular message or circumstance (Chaiken, Liberman, Eagly 1989). As motivations may be contextual and driven by individual difference factors, so too are heuristics relied upon differently and with varying strengths depending on the situation (Chaiken, Liberman and Eagly 1989). In the online economy, where it is all too easy to stumble across an unfamiliar and website, brand famiarity is theorized to play a vital role in determining a data privacy safety and allow for convenience of online shopping/surfing to continue. Brand familiarity may be among the most important heuristics to consider online and the material entities to trust online are the brand websites that consumers frequent, a phenomenon intrinsically linked to mere exposure (Zanjoc 1968).

The Meaning of Brands

This section aims to underline the importance of brands without exhausting the vast amount literature on the topic. In the online economy, the branding has become integral for companies to survive (Aaker and Joachimsthaler 2000; Kapferer 2005). A strong brand is attributed with the ability to increase advertising and marketing effectiveness, making consumers more likely to pay attention to additional communication from the brand with more favorably and the recall the brand with matching affective or cognitive reactions (Keller 2009). A brand can become linked to a set of colors or words and unconsciously processed as associated with that brand (Galli and Gorn 2011), allowing the theorizing that consistent branding may help create an unconscious representation and set of expectations for a brand and allowing for those representations to act as heuristics. As mentioned in the previous chapter, brands are capable of great influence and used as heuristics even overriding senses like taste as noted in the peanut butter with no brand label and peanut butter with brand label example. The peanut butter with a brand label was preferred regardless of the actual peanut butter taste (Hoyer and Brown 1990).

Brand familiarity is as an important heuristic in a complex society over-saturated with information, especially in the online economy. In fact, the perceived risk literature notes that consumers tend to know the risks involved with certain actions and take steps to reduce that risk such as information seeking or relying on a brand image (Sheth and Venkatesan 1968). Sheth and Venkatesan (1968) manipulated perceived risk, and found that information seeking and deliberation about a purchase declined as a result of lack of brand loyalty.

Based on previous studies, familiar brand name will be manipulated because a familiarity is a necessary prerequisite for brand trust. Past experience and the resulting familiarity with any type of organization is the number one reason cited for trusting that organization with personal information (Milne, Rohm and Boza 1999). Brand familiarity and favorable brand name have been found to represent existing knowledge structures from which brand trust is derived and may operate as a judgmental heuristic (Maheswaran, Mackie, and Chaiken 1992). Such a knowledge structure, much like an existing stereotype, may create expectations about a product (Maheswaran, Mackie, and Chaiken 1992). Here, the knowledge structure offers information about brand's relative safety. It is expected that a familiar brand name and thus more trusted brand name may serve as a heuristic cue in the online shopping/surfing environment. For example, an individual may not stop to check the privacy or be wary of their navigation on a brand website with which they are familiar and specifically that they trust. An unknown brand website, because the heuristic rule relied upon for a familiar and liked brand name does not apply to a brand the consumer has not experienced, will likely increase the motivation to get more information about the advertisement's privacy policy and result in higher voiced privacy concerns. It is also theorized that brand familiarity will lessen the perceived risk felt by those in high risk condition and unfamiliar brand is likely to increase feelings of risk in the high risk condition.

Trust

Trust is essential to a functioning society, beginning with its most basic manifestations in daily life (Morgan and Hunt 1994). Here trust is defined as "a generalized expectancy held by an individual that the word of another…can be relied on"

(Rotter 1967, p. 651). This study involves trust of one another, or interpersonal trust and trust of the institutions involved in online behavioral advertising.

General trust in the government, is integral to the functioning of a peaceful and happy complex society where it is not possible to examine every claim of safety a government makes. For example, the Food and Drug Administration is charged with making sure food passes safety inspections and is approved for human consumption. There is error in the agency's judgment as many drugs are recalled and some excite trial lawyers looking for large settlements with the help of injured patients (Maris 2012). Still, in general, people trust that the medicines their doctor prescribes will make them better and they move on with their lives with little thought to the contrary.

The human brain is a considered a limited capacity processer and as such often uses heuristics, such as trust, to make decisions on the daily basis and exert mental energy on less mundane tasks (Lang, 2000). Following this logic, a society with higher institutional trust, or a citizens' general trust in other people and institutions, will likely be both happier and more efficient (Putnam, 1993).

Interpersonal Trust

Nowhere is the bombardment of information greater than it is on the Internet. Understanding the facets of how online data collection works may not only be a seemingly daunting task, but one many people have little interest in understanding. The human brain a limited capacity processor and as such often uses heuristics, such as trust, to make decisions on a daily basis, thus preventing exertion of mental energy on mundane tasks (Lang 2000). It makes sense then that interpersonal trust may serve as a

heuristic for consumers as they navigate the risks and benefits of shopping online as well as the privacy risks involved in doing so.

A personality trait related to a person's trust of others, interpersonal trust has been linked to concern or lack thereof about security online and the likelihood of purchasing online (Das 2003). Interpersonal trust seems a likely antecedent to how people view the risks and benefits of shopping online and the privacy risks associated with online activities. Interpersonal trust here is conceptualized as an enduring psychological state wherein a consumer has the intention to accept vulnerability in reaction to the positive behavior or expectations of the other (Evans 2008; Rousseau 1998). More trusting people are likely to disclose more private information than those who are less trusting (Joinson 2010). In addition, research has found that while there is a disconnect in the lack of self-protective behaviors consumers take to protect their privacy, that high trust predicts lower levels of privacy concern (Joinson 2010). People with high trust levels may focus on the benefits of online shopping because it is just another environment where trusted others are operating. Theoretically, when citizens trust each other, it may seem easier and "more rewarding for them to participate in community and civic affairs" (Zmerli & Newton, 2008, p. 6) which may further be bolstered by institutional trust.

Institutional Trust

As beings in a complex society, our trust in institutions may also be influential on the perception of online privacy risks. Some institutions like governments and industry are charged with influencing societal norms and perceptions through mechanisms of socialization (Freitag 2009). Institutional trust is linked to the maintenance of a cooperative social climate (Zmerli & Newton, 2008) and integral for the efficient

functioning of society. Research by Freitag & Bühlmann (2009) argued that political institutions could foster generalized trust. This study adds to the government, also individual brands, the advertising industry and the individual advertiser to the concept of institutional trust in the realm of online behavioral advertising.

That said, the privacy paradox that exists may exist in part because of trust in institutions. For example, people may generally trust that the Internet is generally safe and that advertisers and the government will work to keep their data safe, so they are left to worry about more motivationally relevant issues. It is theorized that people continue to shop online despite news of data breaches and the known potential for data collection aggregation and abuse because, at the end of the day they trust the institutions charged, in their minds, with regulating such behaviors. This phenomenon is also witnessed in food safety, an issue that would seem, on its face, be quite motivationally relevant. There are dozens of recalls of certain types of foods each year that can cause deathly illness but consumers still flock to the grocer to buy their lettuce and beef trusting it is safe. The United States does have a Food and Drug Administration charged with protecting us, does it not?

The crux of the privacy paradox is that despite consumers' calls for more privacy protections and complaints that they have lost control over their personal data online, evidence suggests they do little or nothing to protect that privacy and in fact, disclose far more information in reality than they say they will when asked by researchers (Norberg, Horne and Horne 2007; Nowak and Phelps 1992) and few opt-out of tracking technologies (Winkler 2001). It might be that consumers are motivated by social acceptability perceptions (response bias) to express privacy concerns when asked on a

survey questionnaire or in a lab setting (Milne 1997). The social desirability bias accumulates over time and through cultural norms leading groups of people to respond to certain issues in similar ways (Haidt 2012). It is likely that the cultural norm in our society is that privacy is a value that should be preserved and thus, most people simply select the desire for additional privacy (regardless of what that word may mean in reality) in line with the current American culture. However, once immersed back into the real world, consumers continue to behave as they had before, ignoring privacy policies and agreeing to terms of use on websites with no so much as a second thought. The idea that people trust in the very institutions they site as needing regulation, until perhaps something very embarrassing or inconvenient were to happen to their data, and regain their complacency in the comfort of that notion. That behavioral intentions in the realm of online privacy research have not accurately predicted actual behavior (Norberg, Horne and Horne 2007) is the piece of the privacy paradox issue we seek to explain through the lens of the Heuristic-Systematic Processing Model (Chaiken 1980) and especially, through the use of institutional trust, as a powerful heuristic in the e-commerce context and one theorized, here, to offer a reason why people may say they want protections and feel risk to their online data but do nothing to remedy the situation in everyday life.

Previous research on acceptance of new technologies (e.g., gene therapy) notes that new technology is reliant on "consumer shopping behavior and political regulations" to determine its use in the future (Siegrist 2000, p.195). Data collection online and its use in online behavioral advertising, like all new technologies, is also subject to the habits and preference of consumers and of course must operate within the boundary of governmental regulations. Trust in institutions has been theorized to be a useful coping

mechanism for the consumer who has a lack of knowledge in a new technology or experience (Siegrist 2000). This trust could be developed in a myriad of ways but some researchers have noted that previous experience purchasing from a company or product familiarity may lead to the likelihood of repeat business (Milne 2009; Sheehan and Hoy 2000). In accordance with the findings that previous experience may predict future behavior, internet users are more trusting that non-internet users (Hampton 2011). We theorize that our participants have likely purchased items online and surfed online often, thus increasing their trust in institutions involved in such transactions, namely: advertisers, the advertising industry, individual brands and the government. For example, if a consumer is shopping online and is ignorant of the process that allows a book similar to the one they have just chosen on Amazon.com to be suggested, the suggestion is not likely to increase perceptions of online privacy risk or online shopping risk because the consumer trusts Amazon.com or online retailers, in general because of previous experience. Several previous studies have found "a negative association among perceived risk and trust in experts, government and industry" (Siegrist 2000 p.196).

Online Advertising Context

Behavioral Targeting and Data Privacy

Behavioral advertising, and how consumers perceive it, has been central to the public debate on consumer privacy. Online behavioral advertising ("OBA" for short), broadly speaking, refers to tracking an individual's online activities in order to deliver advertising tailored to the individual's interests (FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising 2009).

Behavioral advertising first received national attention in late 2008 when U.S.Rep. Edward Markey, D-Mass., held hearings on deep packet inspection

technology("DPI")—a process by which a user's Internet service provider (ISP) allowed an advertising network access to all of the user's activities, and an advertising network then directed ads to that user, directly targeting the user's interests suggested by his or her browsing activities. Soon after it received national scrutiny, DPI largely faded away, and the public focus shifted to other behavioral advertising programs.

First party online behavioral advertising, which is common, involves behavioral ads placed on a website based on the consumer's browsing activity *on that website*. An Internet user browses a website, and the website generates one or more "cookies." "Cookies" are data phrases which gather and save information about a user's preferences, so that different web applications can tailor their information to those preferences. They allow users to save particular page designs and content, to save and correctly place usernames and passwords, and to utilize "shopping cart" programs at e-commerce sites.(FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising 2009, 26). Cookies are central to most OBA. To take an oversimplified example, a user of the mythical usasports.com website who checks baseball scores and articles may prompt that website to post a cookie to the user's computer, noting that interest. The website operator, thereby knowing the users baseball interest, may then divert baseball-related content and ads to the user. Similarly if the user made purchases through the website's e-commerce application, cookies may be generated and posted based on those purchases.

First party OBA has been generally viewed as acceptable. In its February 2009 report, the FTC staff defined OBA to encompass only the activities that it felt needed supervision and possible regulation, and it excluded first-party behavioral advertising

from that definition. The FTC staff noted that in first-party OBA no data is shared with any third parties, and it found the practice generally appropriate and permissible: "The staff agrees that first party behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites"(FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising 2009, 26) Put simply, users generally are assumed to trust the websites they frequent, and to understand that that trusted websites will monitor their activities, and post related content in response to the user's apparent interests.

Third party online behavioral advertising—behavioral advertising placed on a website based on a consumer's browsing activity on an *unrelated site*—takes behavioral advertising to the next step. This practice has been the focus of regulatory and Congressional attention since late 2008. In third party behavioral advertising, the suppliers of behavioral advertising (chiefly advertising networks) collect and use consumer information across various websites by placing "cookies" on user computers, and then generating ads in response to what they know about the consumer identified by the cookies. That is, because of information learned about a user's activities on website A, targeted interest-based ads may be placed to that user weeks later, when he or she is visiting unaffiliated website B.

Ad networks place their behavioral ads based on information about particular users' browsing activities. More precisely, they use cookies to identify users with certain interests, as revealed by past browsing activity. As an example, a user of usasports.com who frequently views hockey-related content on that website might be presented with

hockey-related ads when he or she browsed unrelated websites. That would occur because an ad network allied with usasports.com initially recognized the user's hockey interest, and placed a cookie on his computer. Then, when the consumer visits another website, the ad network was able to place a hockey-related ad there, knowing that hockey was one of the consumer's interests. Although oversimplified, this example describes how advertising networks work—they take note of user interests as found on various websites, and they then arrange for posting of targeted ads when those users visit websites where the ad networks have contracts to place ads(Kahn 2007). The FTC has so far concluded that this kind of cookie-based behavioral advertising across unaffiliated websites should be subject to either government regulation or robust self-regulation (FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising 2009; Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers 2010).

The Federal Trade Commission is charged with the regulation of advertising and has historically conceptualized privacy as the control a consumer has over transactions involving information between individuals and others (Sheehan and Hoy 1998). Online behavioral advertising has made consumer control over such transactions more difficult. First party advertising involves a website using consumer data to make suggestions within the site available to the consumer (e.g., a consumer puts a book in their cart at an online bookstore and other books are suggested based on that selection). Third-party advertising involves the consumer click stream data and purchase behavior online to be aggregated and used to show products and advertisements of interest to consumers on sites apart from the ones they initially viewed. The FTC is more concerned about third-

party advertising because the potential for consumers to become confused about how their data is being used and as a result has made suggestions to the advertising industry in the effort of making consumers aware of the practice and to increase informed decision-making on their behalf. According to the agency, "Every Web site where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that data is being collected to provide ads targeted to the consumer and give consumers the ability to choose whether or not to have their information collected for such purpose (FTC 2007)."

In an effort to prevent the creation of Federal Trade Commission regulations, the advertising industry has worked to provide regulatory logos on advertisements generated through the use of consumer online behavioral data based on the FTC's notice provision based on the idea that consumer control over data is a feature of privacy (Sheehan & Hoy, 2000).

The icons, when clicked, offer information about how to opt-out of targeted advertising services and how the advertisements are generated. The use of warning labels have been used to offer consumers the chance to make informed decisions about purchase and usage of products, an activity considered inseparable from a free-market system (Cox III, Wogalter, Stokes, & Tipton Murff, 1997). However, the studies on the effectiveness of warning labels have been inconsistent (Cox III, et. al., 1997). The issue with privacy seals is that they have often been interpreted by consumers, not as a gateway to additional information, but as safety seals (LaRose & Rifon, 2006).

The mere presence of a privacy policy easily visible on a website may be enough to increase consumer trust in the site regardless of the content of the policy (Pan and

Zinkhan 2006) belying the fact that most people don't read the policies but simply rely on them as a heuristic cue denoting safety. The Digital Advertising Alliance's use of the AdChoices icon on behaviorally targeted ads online have been shown to increase the consumer's click-thru rate. Over half of those surveyed said they would be more likely to click on an ad with the icon and upwards of 73 percent said they were more comfortable with advertisements that followed the privacy policies of the Digital Adverting Alliance's self-regulatory program (Bachman 2013). The article is silent on the number of people who actually read and understood the privacy policy offered by the DAA however previous research has noted that few people read privacy policies or choose to opt-out (Langenderfer and Miyazaki 2009).

The mere fact that research has shown that consumers are unlikely to read the privacy policy but that the presence of a logo denoting safety of some sort may increase trustworthiness and decrease perceived risk is enough to point to the idea that unless motivated by a personally relevant threat to their data, consumers are unlikely to actively search for information that may lead to their increased control of their personal data. The effectiveness of the icons or privacy policies will not be assessed in this study but it is worth noting the efforts by the industry to inform consumers of privacy issues with online behavioral advertising as context.

The Privacy Paradox, Some Context

The privacy paradox or the voiced desired by consumers for privacy protection and rights but the limited or non-existent measures of self-protection consumers take in the area of data collection is not a new phenomenon. Nowak and Phelps and others noted as early as 1992 that many consumers support privacy protection measures,

including restrictions on information exchanges (Nowak and Phelps 1992; Wang and Petrison 1993). However, the high level of consumer privacy concern appears to have no significant impact on consumers' shopping behaviors. Most consumers are willing to give up some of their privacy to participate in the online economy (Norberg, Horne and Horne 2007; Nowak and Phelps 1992).

The reasons for this paradox have rarely been outlined and represent an understudied area but some theories have been put forth to describe the reasons behind the paradox such a perceived behavioral control or the idea that consumers are required to provide personal information to participate in the online economy and thus have relinquished control in order to participate, they may not have the knowledge to comprehend when and how to withhold information online, some may fall prey to immediate gratification or have limited time to fully think through the consequences of providing information (e.g., signing up for the chance to win a boat may result
in mailings from boat dealerships) (Yap et. al. 2009). Finally, consumers may have become accustomed to the idea of providing information to retailers and a habit forms (Yap et. al. 2009), a theory that supports the idea that familiarity with the process of online shopping leads to lower privacy concerns and more information disclosure to retailers and marketers, a finding shown across cohorts (Milne, Gabisch, Markos, and Phelps 2012). Thus, each age cohort has shown lower privacy concerns with information disclosure as Internet use in each cohort increased.

Currently, there is no empirical support to suggest one theory's superiority over another, although some research corroborates the idea that familiarity with the online economy and the brands that inhabit it may play an important role in decreased privacy

concerns (Sheehan and Hoy 1999; Chaiken and Maheswaran 1994). In other words, brand familiarity is theorized to reduce privacy concerns in the online economy because it is used as a heuristic tool by consumers to reduce cognitive load and make decision faster and more efficiently. The current study theorizes that under normal, everyday online browsing and shopping conditions, the consumer relies on heuristics (such as institutional trust and brand familiarity) to guide his judgments about privacy issues that may lurk on the Internet and only when asked about their concerns or made to feel a personal risk about their data, will they take self-protective measures (e.g., seek additional information) and/or voice concerns about their data privacy, a type of social desirability bias (Milne 1997).

Privacy in an Online Advertising Context

One of the reasons the balance between consumer perceived expectations of privacy in the online behavioral data collection context and the interests of advertisers and marketers has been so difficult to strike is that consumer privacy interests are malleable and situational. Privacy is a concept that suffers from an embarrassment of meanings in the offline world (Solove 2006). When dealing with the aggregation of click-stream data or online behavioral data, the issue is even more abstract. As a result, this study will work from two definitions, one legal and one behavioral. However, it is important to note that these definitions of the privacy concept in online behavioral data collection context are not mutually exclusive and work to inform one another. The legal definition of privacy is the reasonable expectation a consumer has that the act, words, etc. that is at issue should be kept from (Solove 2006). Then following from the legal definition is the consumer's perceived expectation of privacy or the claim a consumer

makes over what information about himself or herself should be known to others (Westin 2003). The behavioral definition was derived from Westin (1967) who said that people have the right to decide when, how, why and to what extent they will share information, a notion of control over personal information. He notes that this is a process that is socially constructed by culture and is constantly being renegotiated.

A brief history of the privacy beginning from a biological and moving to a legal concept will be offered as a way of exemplifying the complexity of nailing down a precise conceptualization of the consumer's perceived expectation of privacy when it comes to online behavioral data.

Westin (1967) in his book on privacy, noted that its roots are biological. Interestingly, he notes that barnyard cattle, birds on a telephone wire and wild animals all stand a certain distance a part, a space attributed to privacy. In fact, the beautiful song once attributed to birds who simply love to sing may actually be a call for privacy or to keep others from their territory (Nelson and Croner 1991).

Humans also have privacy stemming from biological bases. There is always a constant balance that must be struck between privacy and the need to be stimulated by other human beings/species of your own kind. The way privacy manifests in the human world is described by Westin as comprising four distinct types of privacy. They are described roughly as solitude (being completely away from other people), intimacy (being close to friends/family), anonymity (this is equivalent to being a stranger walking amongst people in a town in which you know no one), and a psychological privacy (not being as open with one's thoughts). Interestingly, violations of any of these types of privacy can be harmful to the human psyche. For example, those whose psychological

privacy has been invaded (e.g., their thoughts, ideas, deeds, etc. spewed across the news) can lead to suicide. We have seen this with high profile people. When their secrets are exposed, a sense of control lost – they occasionally commit suicide (Fuchs 2012; McRoberts and Simpson 2002).

The role of the consumer in protecting her data has been emphasized because control of where and how one's data is used is an essential part of the concept of consumer privacy online and thus, consumer advocates have urged the growth of consumer knowledge in this area (Foxman and Kilcoyne 2001). Though it makes sense that increasing knowledge of how data is collected and how it is used to serve relevant advertising may reduce the voiced concern about data privacy and the desire for more privacy protections, actual knowledge is at best a weak predictor of privacy concerns (Smit, Van Noort, and Voorveld 2014; Shoenberger and Thorson 2014; McDonald and Cranor 2010). In fact, knowledge of the intricacies of a new technology is typically a weak predictor of concern about or support for the new technology (Brossard, Scheufele, Kim and Lewenstein 2009). Thus, here we do not hypothesize that knowledge of OBA is a relevant variable in our analyses.

Different types of information may be considered more important than others. For example, consumers may be more likely to be concerned about medical and financial information being shared with others than they are about clickstream data being collected (Nowak and Phelps 1992). Also, it is likely that the idea of other people looking at information collected would be considered more of an invasion of privacy than an algorithm putting together information using unidentified online behavioral data, but again, knowledge of this phenomenon seems to have no effect on behavior.

Westin (1967) also talks about how different societies handle privacy. For instance, American households have separate bedrooms for parents and children whereas some cultures sleep side by side or have only mosquito netting in-between the parents and children. Privacy in the latter culture tends to come from a psychological source or not being as open with one's thoughts (and taking to the woods for times when intimacy is intended) (Westin, 1967). The American culture derives privacy from physical space delineations. Westin wrote his book during a time when the biggest technological threats were lie detector tests and wiretapping which he thought may intimately invade personal privacy. His concern was mainly for the ability for technology to increase surveillance and to be used by the government. Indeed, an excerpt from Humphreys (2011) it was noted that any information society or high tech society was in fact, a surveillance society.

In their famous law review Warren and Brandeis (1890) were also concerned about the potential for surveillance from the government with the advent of new technologies. They noted that what was once whispered behind closed doors would one day be screamed from the rooftops. Their concerns seem to echo those of consumer advocates today who worry that information people put online and the behavior that is tracked is capable of inferring identification and eventually leading to profiles of an individual that may exist online and exist with error, leading to minor consequences such as price discrimination and serious ones, employment discrimination (Podesta et. al. 2014; Turow, Feldman and Meltzer 2005; Marcoux 2012).

Distilled from the Warren and Brandeis law review, the first to mention a potential right to privacy which had not been included in the Constitution or the Bill of Rights, was the idea that a citizen has the right to "be left alone." It wasn't until 1965 in

the case of Griswold v. Connecticut that the court suggested that citizens of the United States had a constitutional right to privacy found within the matrix of amendments. The case involved the dissemination of birth control to married couples and it was found that this was within the realm of their marital privacy. The judges noted that zones of privacy existed under what was eloquently named "penumbras." However, the aggregation of click-stream data has not been clearly covered under the zones and leaves it largely free from the reach of legal remedies, thus consumers have no legal right to exert control over the use of that data (Rotfeld 2009).

The United States is in a in a phase now where the law can try to build boundaries to protect violations of privacy or under the definition struck here, control over their clickstream data online, but first privacy boundaries have to be established by consumers and articulated to regulators using sound empirical research. Beginning to discover those boundaries begins with understanding the limits of consumers' expectations of privacy in the online economy, what drives them to view their data exchanges as potentially risky and what underlies the privacy paradox.

The issues that arise as the result of the use of a socially constructed and contextual definition of privacy as it applies to the online economy, essentially when and where a consumer should have the right to informed consent about how to control their clickstream data, will be studied through the lens of Shelly Chaiken's Heuristic-Systematic Model

Institutional trust, while controlling for the manipulations and interpersonal trust is expected to do the same.

3. HYPOTHESES

The primary question guiding this study was whether heuristics are guiding consumer behavior in the online economy. Thus the following hypotheses are proposed:

Participants randomly assigned to the high risk group are theorized to be more likely to systematically process information offered on the scenarios' websites. Additionally, they will be more likely to desire more regulation, perceive greater online privacy risk, perceive less control over their data online and search for information about how to protect their privacy in the future. Thus:

H1: Those in the "high risk message" group will be more likely to report (H1a) higher perceived online privacy risk, (H1b) higher desire for regulation of online privacy, (H1c) express less perceived control over their data online, (H1d) higher intention to search for additional information about privacy on the website information on the website in general, (He) higher intention to search for additional information on the website in general, (H1f) higher intention to search for information to protect their privacy in the future than those in the "low risk" group.

Brand familiarity is expected to act as a heuristic cue, denoting safety and offering a short-cut for consumers to rely on when they are in the online economy. Thus, brand familiarity is expected to mitigate the effects of high risk on all of the dependent variables: reduce perceived online privacy risk, reduce desire for regulation, increase the perception of control over data online, decrease the desire to search for information in general and about privacy on the scenarios' websites, and decrease the desire to search for information to protect data privacy online in the future. Thus:

H2: When the brand name associated with a website is familiar those in the "high brand familiarity" group will be more likely to report (H2a) lower perceived online privacy risk, (H2b) lower desire for regulation of online privacy, (H2c) express more perceived control over their data online, (H2d) lower intention to search for additional information about privacy on the website information on the website in general, (H2e) lower intention to search for additional information on the website in general, (H2f) lower intention to search for information to protect their privacy in the future than those in the "low risk" group.

H3: Level of manipulated brand familiarity and level of manipulated risk will interact in the following ways: (H3a) high brand familiarity will decrease perceived online privacy risk in the high risk group, (H3b) high brand familiarity will decrease desire for regulation of online privacy in the high risk group, (H3c) high brand familiarity will increase perceived control over their data online in the high risk group, (H3d) high brand familiarity will decrease intention to search for additional information about privacy on the website information on the website in general in the high risk group, (H3e) brand familiarity will decrease intention to search for additional information on the website in general in the high risk group, and (H3f) brand familiarity will decrease intention to search for information to protect their privacy in the future in the high risk group.

Further, predicting above and beyond the manipulations of risk (high/low) and brand familiarity (familiar/unfamiliar) are the measured individual difference variables of interpersonal trust and institutional trust. The trust in others, as a trait, may work as a heuristic over and above the risk manipulation and brand familiarity as a heuristic because of its importance for a person to move through her day without needing to

evaluate every person she may encounter (Joinson 2010). Thus, over and above the manipulations it is expected that interpersonal trust will predict reduced perceived online privacy risk, reduced desire for regulation, increased the perception of control over data online, decreased the desire to search for information in general and about privacy on the scenarios' websites, and decreased the desire to search for information to protect data privacy online in the future.

H4: Higher interpersonal trust will predict while controlling for brand familiarity and level of manipulated risk (H4a) lower perceived online privacy risk, and (H4b) lower desire for regulation of online privacy, (H4c) higher perceived control over data online, (H4d) lower intention to search for privacy information on the scenario websites, (H4e) lower intention to search for additional information on the website in general and (H4f) lower intention to search for privacy information in the future.

Institutional trust is linked to increasing interpersonal trust and also essential for the efficient functioning of society (Freitag 2009). Previous studies have linked trust to online disclosure behavior (Norberg, Horne and Horne 2007) and here, institutional trust, like interpersonal trust is expected to predict over and above the manipulations of risk and brand familiarity and because it has been considered a precursor to interpersonal trust (Freitag 2009) it is also expected to predict beyond interpersonal trust. Thus:

H5: Higher institutional trust (here, in individual advertisers, the advertising industry, individual brands and the government) will predict while controlling for brand familiarity and level of manipulated risk and interpersonal trust (H5a) lower perceived online privacy risk, and (H5b) lower desire for regulation of online privacy, (H5c) higher perceived control over data online, (H5d) lower intention to search for privacy

information on the scenario websites, (H5e) lower intention to search for additional information on the website in general and (H5f) lower intention to search for privacy information in the future.

4. METHOD

Pre-Test

The pre-test of the 2 (familiar brand/unfamiliar brand) x risk (high/low) x 4 (2 familiar brands and 2 unfamiliar (fake) brands) was run between subjects. Between-subjects designs may reduce the potential influence of other treatment levels on participants' processing and responses (Reeves and Geiger 1994) and was chosen due to the possibility of participants' guessing the manipulation. The experiment was conducted using a population of staff members recruited from a large Midwestern University via an email announcement in an effort to determine the effectiveness of the language of the risk used in the high risk condition. Brand familiarity was another of the manipulation checks integral in the pre-test. Participants were offered a chance to win $50. There were 76 participants, 8 male and 68 female. The average age of this sample was 43 years old. These participants indicated spending on average, at least 2-3 hours a day online, M=4.19, *SD*= 1.79 (where 4= 2-3 hours per day) and the average time spent shopping online each day was less than an hour M=2.00, *SD* = .52 (where 2=less than an hour per day). All 76 participants indicated they had made at least one purchase online in the past month, M=3.93, *SD*= 1.59. See Appendix 1 for the pre-test questionnaire in its entirety.

Pre-test manipulation checks

Manipulation checks were calculated in an effort to determine whether the manipulations were successful. For both manipulations, the test statistic showed significant differences between the means, where those in the low risk condition reported

less risk and less concern, and those in the low brand familiarity condition reported significantly lower brand familiarity than those in the high brand familiarity condition.

An independent samples *t* test demonstrated that participants in the high risk condition perceived greater sense of personal risk (M = 3.68, SD= 1.00) than those in the low risk condition (M= 2.68, SD=.75), t =4.88, p <.001. An additional independent samples *t* test demonstrated that participants in the high risk condition perceived greater sense of concern (M = 3.58, SD= 1.10) than those in the low risk condition (M= 2.70, SD=1.0), t =3.63, p <.05. The results of the pre-test manipulation checks determined that the high and low risk messages would be retained for the main study.

An independent samples *t* test demonstrated that participants in the high brand familiarity condition perceived greater brand familiarity (M = 4.27, SD= 1.10) than those in the no familiarity condition (M= 1.00, SD=.00), t =25.83, p <.001.

The results of the pre-test manipulation checks determined that the high and low risk messages would be retained for the main study. It also indicated that the "real" brands selected were significantly more familiar to the participants than the fake brands.

Main Experiment

Participants

Three hundred participants were recruited from an online survey provider, Mechanical Turk (MTurk) at Amazon.com. People can sign up to be "workers" through Amazon.com. They can choose to participate in any survey/online experiment for which they qualify. As compensation, participants were offered $1.00 Amazon credit provided through the Amazon marketplace. The campus IRB approved of the recruitment methods and payment plan. MTurk is a relatively popular tool to collect population data through an online platform, even though validating MTurk data for research use has just begun

(Buhrmester, Tracy, & Gosling 2011; Simnos and Chabris 2013). The allure of MTurk for the researcher is the accessibility to participants and the reasonable price at which responses can be gathered. MTurk workers indicate that earning additional money motivates their work while 4% of them state that it is a primary source of income (Paolacci et al. 2010). However, MTurk participants produce reliable results that are consistent with previous decision- making research (Goodman, Cryder and Cheema 2012) and exhibit similar judgment and decision biases compared with online discussion board participants (Paolacci et al. 2010). Buhrmester et al (2011) asserted that MTurk participants were more demographically diverse and more representative of non-college populations than those of typical Internet and traditional convenience samples. Simnos and Chabris (2013) compared data collected from MTurk to data from a nationally representative telephone survey. Their results indicate that an MTurk sample reflected a nationally representative sample of the United States population as the pattern of results for a self-selected MTurk sample closely matched those of their random telephone survey. MTurk has an option to use "Masters" only or people who have completed N number of surveys and received a certain quality score. This study did not include only Masters as participants in an effort to include those who may not share the biases of those who essentially take surveys for a living. This effort was based on an assumption by the researcher and not on actual data

The number of participants used was determined using an a priori power analysis G-Power analysis software (Faul, Erdfelder, Lang and Buchner 2007). The software concluded that the sample size needed to detect a small-to-medium effect (f=.2) for an F test on a between-subjects factor and interactions at an alpha of .05 with four groups was

estimated to be 199. Due to the researchers' lack of familiarity with MTurk and the possibility of needing to remove quite a few participants due to incomplete questionnaires or other issues, the sample actually collected was larger.

The ease of MTurk allowed for over-sampling in the case that some of the participants had to be removed due to incomplete questionnaires or insincere participation. Insincere participation was quantified by the time people took to complete the study. It seemed unreasonable for any person to take less than five minutes when the average was close to 15 minutes. Thus, people taking less than five minutes were rejected. The links were assigned randomly and some conditions received more participants than others as a result. Participants were removed from the dataset and rejected from the MTurk payment for either taking too little time (5 minutes or less when the average time to complete the survey was 14 minutes and 39 seconds), not entering the survey code found at the conclusion of the survey or in Qualtrics for significantly incomplete questionnaires. Twenty-three people were rejected due to insincere participation (taking 5 minutes or less or not supplying the survey code at the conclusion of the questionnaire) and four were removed from the Qualtrics dataset for substantially incomplete questionnaires. The four deleted from the Qualtrics dataset were deleted based on substantial blanks on questions (10 or more blank questions). The resulting N=287. Although participants did not receive credit for their M-Turk for insincere participation, the completion of their dataset as unknown until examining the datasets in Qualtrics. This is because forced responses were not approved by the IRB in an effort to allow participation to remain voluntary at every stage of the study.

The average age of the sample was 35 with 52 % female participants and 48% male participants. Just over 87% of the participants indicated that they had completed at least some college. At least 87 % of the sample indicated encountering advertisements based on items they had previously searched for online, M=3.48, *SD*=.93 (where 1=never and 5 = always) and 26.8% indicated clicking on advertisements that offered discounts, M= 1.99, *SD*= .86 (where 1=never and 5 = always). Over 63% of the sample indicated spending four or more hours online each day M=5.36, *SD*= .96 (where 5=3-4 hours a day) and 93% indicated they had made at least one purchase online in the past month, M= 3.73, *SD*= 1.53. When asked if they had read the privacy policies that appeared in the scenarios they viewed, most indicated they had not: Walmart.com: M=2.65, *SD*=.74; BestBuy.com: M=2.71, *SD*=.65; SuppliesPlus.com, M=2.94, *SD*=.32; CamerasGalore.com, M=2.94, *SD*=.32 (where 1=yes, 2= I don't know, and 3= No). Please see Appendix 2 for the questionnaire used in the main experiment in its entirety.

Procedure

The experiment took place online using a combination of MTurk crowd sourcing and Qualtrics survey software. Participants were recruited through MTurk's marketplace and self-selected to take the study and once they selected the study, it was administered via a link hosted by Qualtrics.com. There were four conditions. Participants were randomly assigned to one of the condition links.

First, the participants were shown the information disclosure instructions required by the IRB. They proceeded to answer demographic questions and questions about their online shopping habits (e.g., how often they shop online, how often they click advertisements that offer discounts for a product, how often they use Facebook, etc.).

After completion of the demographic and shopping/surfing habits, the participants saw a screen that said, “Please wait while we calculate your risk quotient.” A ten second counter counted down on the page and at the conclusion of the countdown, participants randomly saw the high risk message or the low risk message.

The main stimulus was meant to induce perceptions of information insufficiency by means of a personally relevant message that raised concern about data privacy issues. The high risk group received a sign after completion of the demographic section that read: Based on the information you provided, you are at HIGH RISK of your data being stolen or used in a way you find embarrassing or inappropriate. In line with the most effective messages according to Turner and colleagues (2009) in the health communication research, the message had another component: One way you can reduce your risk is to fully understand a website’s privacy policy before clicking through its pages or making a purchase (please see Appendix for an example of both the high and low risk messages).

After the exposure to the high risk message (low risk message) the participants were given two scenarios. All participants received two familiar brand or unfamiliar brand scenarios of items similarly priced to avoid confounds that price may add to the experiment. Participants were instructed to imagine they were going to purchase either a camera for $500 from Bestbuy.com or CamerasGalore.com or a bicycle for $650 from Walmart.com or SuppliesPlus. After viewing this page, the participant was directed to click to the next page which said: Please click the type(s) of information you would want to check before ordering your camera/bike from this site. The options for this section were derived from the actual sites used, Bestbuy and Walmart and included: How to

place an order, information the website collects about you, use of cookies on the website, rebates, how the site uses pattern recognition to link your purchase history to products you might life, information the site exchanges with third party advertisers, defective items, exchanges, refunds, return exceptions, how the site uses your credit card information, order processing time, how to opt-out of the site's cookie tracking system, how the site ensures consumer data privacy, the website's mobile application privacy options, contact information in case you have privacy related questions, a pledge of accountability by the company, how your IP address and other information are collected by social media widgets on the site (for example, Facebook or Pinterest icon), customer reviews about the site, and a privacy seal or icon. For example, E-Verify or Better Business Bureau icons.

At the conclusion of the scenarios, the participants filled out questions about information they would like in the future and the remaining questionnaire including measured items such as brand familiarity, perceived risk to data online, and perceived control over data. Participants were thanked for their time. As required by IRB due to the deceptive nature of the study, participants were given the opportunity to withdraw their click-through data if they would like after learning the true purpose of the study. There were no participants who indicated a desire to withdraw their answers.

Manipulation Checks

Brand Familiarity. Participants will note how familiar they are with the brand that they are exposed to with one question on a 7 point scale: "How familiar are you with the real/fake brand?" Based on a previous study (Campbell & Keller, 2003).

Risk perception. Participants will on a 7 point Likert scale how much personal risk they felt after being told they were in the high risk group.

Measurements

Demographic items: Age, gender, education level (main test), income (main test), how often do you surf online? How often do you shop online? How confident are you that you understand how online behavioral advertising works (ie. When you see an advertisement on another webpage clicking or searching for the item/brand advertised?) How often do you click advertisements that offer discounts for a product? How often do you use Facebook? Some of the questions are, of course, unnecessary to the analysis but serve the purpose of setting the participants up for the main manipulation.

Institutional Trust. Trust in institutions was measured using a scale adapted to the issue of online data collection used to create online behavioral advertising (Siegrist 2000). The scale consists of four items measured on a 7-point Likert scale. Following the prompt of "How much do you trust the following institutions or persons in terms of how well they fulfill their responsibilities in collecting and handling consumer data collected online?" the four items included: the government, individual advertisers, the advertising industry and individual brands.

Interpersonal Trust. Conceptualized in this study as a personality trait related to a person's trust of others, interpersonal trust was measured with an established scale consisting of five items measured on a seven-point Likert scale (Das 2003). The items included, " In dealing with strangers one is better off to be cautious until they have provided evidence that they are trustworthy," "If you are not careful, others can easily manipulate you." "Most repairmen will not overcharge even if they think you are ignorant of their specialty." α = .75.

Dependent Variables

Amount of general information desired. Systematic processing is operationalized an effortful information search/desire for information. When individuals seek out information in order to increase their confidence in a particular judgment, systematic processing is said to be at work (Chaiken, Liberman and Eagly 1989). The items were presented at the conclusion of each scenario with the following prompt" The following information is available on the (brand's) website. Please indicate how likely you would be to seek out and read the following pieces of information before clicking through the website and choosing your new camera/bike. There were two factors used for the general information search. The first was entitled: ***Refund Search.*** Conceptualized as searching for general information about the site but operationalized as a scale comprised of "defective items," "exchanges," "refunds" and "return exceptions."α=.964. ***Ordering Search.*** Conceptualized as search for general information about the site but operationalized as a scale comprised of: "how to place your order" and "payment options." r=.711**.

Privacy Information Search. Because the risk manipulation is specifically designed to alert individuals to the risk to their data online, the items dealing with privacy will also be made into a scale and analyzed as an indicator of systematic processing of privacy information separately. Participants were asked at the conclusion of each scenario: The following information is available on the (brand's) website. Please indicate how likely you would be to seek out and read the following pieces of information before clicking through the website and choosing your new camera/bike: "How secure the website is," "Information the website collect about you," "Use of cookies on the website," "How the site uses pattern recognition to link your purchase history to products

you might like," "Information the site exchanges with third party advertisers," "How the site uses your credit card information," "How to opt-out of the site's cookie tracking system," "How the site ensures consumer data privacy," "The website's mobile application privacy options," "Contact information in case you have privacy related questions," "A pledge of accountability by the company," "How your IP address and other information are collected by social media widgets on the site (for example, Facebook or Pinterest icon)." $\alpha = .982$.

Online Privacy Risk. Perceived online privacy risk was conceptualized as the perceived privacy risks associated with shopping online and using the internet, in general. The scale consisted of four items asked on a 7-point Likert scale. The items included "Data used to serve relevant advertising may be compromised," "Data companies collect about me could end up in the hands of criminals," "Data companies collect about me might be used in ways that make me feel uncomfortable," and "Once my data is collected, I have no control over how it is used." $\alpha=.827$.

***Desire for Regulation*.** This variable is conceptualized as the voiced desire for privacy regulations surrounding online behavioral data usage. Participants will be asked to indicate their level of desire for additional regulation using a seven-point bipolar scale asking Please indicate your level of agreement with the following: " Regulators should do more to protect my data online," "I am concerned about my privacy online," "I would like to know what safeguards are in place in the event of a data breach," "I would like to know how I may be compensated in the event of a data breach," "I would like to know what companies are doing to keep my personal data secure," "I would like to know what the federal government is doing to keep my personal data secure," "I would like to see

additional regulation enacted to protect my data privacy online," "I would like a new law enacted to protect my data online." α=.933.

Perceived Control Over Data. Perceived control over data is conceptualized as the amount of control a participant believes they have over their data online. Participants will be asked to rank statements on a 7 point scale (strongly agree/strongly disagree). "I feel that I have control over my data online." "I believe I can opt-out of allowing advertisers and companies to collect my online behavioral data (ie. Remembering what sites I visit, remember what I click on in those sites to serve advertising that they believe will be more relevant to me)." "I can use online privacy tools to remain anonymous online." "I understand how my online behavioral data is used online." α=.766.

Future Privacy: This variable was conceptualized as another potential symptom of systematic processing or information search. It was operationalized by a scale of two items. The prompt for this set of items was: Please indicate how likely you would be to do the following before clicking through a website in the future: "Choose not to register with a site because it asks for too much personal information, "Search for instructions about how to protect yourself on the web." r=.540**.

5. RESULTS

It was theorized that people in the high risk group would systematically process website information by reporting a desire for additional information about how their data is used and other information about the site and perceive greater privacy risk. Hierarchical regression analyses were calculated to test hypotheses 4-5.

Manipulation checks

Manipulation checks were calculated in an effort to determine whether the manipulations were successful. For both manipulations, the test statistic showed significant differences between the means, where those in the low risk condition reported less risk and less concern, and those in the low brand familiarity condition reported significantly lower brand familiarity than those in the high brand familiarity condition.

An independent samples *t* test demonstrated that participants in the high risk conditions perceived greater sense of risk (M = 3.03, SD= 1.59) than those in the low risk condition (M= 2.44, SD=.85), t =4.99, p <.001. An additional manipulation check meant to measure feelings of risk as a result of the manipulation was also conducted. An independent samples *t* test was demonstrated that participants in the high risk conditions perceived more concern (M = 2.97, SD= 1.27) than those in the low risk condition (M= 2.30, SD=.84), t =5.23, p <.001.

An independent samples *t* test demonstrated that participants in the high familiar brand conditions indicated higher brand familiarity (M = 5.60, SD= .73) than those in the low brand familiarity condition (M= 1.20, SD=.63), t =83.96, p <.001.

Main Hypotheses

Hypotheses 1-3 were tested by means of a series of two-way Anovas. In each of the tests, the independent variables were manipulated risk (high, low) and brand familiarity (high, low).

Main effects of risk

Hypothesis 1a suggested that people would more likely to indicate feelings of Online Privacy Risk in the high risk message group (for a list of items making up the factors, please see Table 1). This hypothesis was not supported, $F(1, 283) = 5.27$, $p<.05$, $\eta 2 = .017$. Interestingly, the high risk group had a lower mean than the low risk group M= 5.29 *SD* = 1.11 (high risk), M=5.52, *SD*= .99 (low risk). This could be a result of the types of questions asked as they reflect a more general risk online instead of a personal risk felt by the participant.

Hypothesis 1b suggested there would higher Desire For Regulation of online privacy in the high risk group. This hypothesis was not supported. In fact, it appears that in the high risk group, people are less likely to desire additional regulation, F (1,284) $=7.20$, $p<.05$, $\eta 2 = .024$. M = 5.51, *SD* = 1.26 (high risk), 5.87, *SD* = 1.04(low risk). Again, it could be that people saw the no need for regulation as a result of their own high risk because that risk was a result (they were led to believe) of their own doing.

Hypothesis 1c suggested that people would feel less Control Over Their Data Online in the high risk group than in the low risk group. This hypothesis was not supported F (1, 284) = 2.50, p=.115, $\eta 2= .01$, r = .07. M=4.52, *SD*=1.43 (high risk), M=4.82, *SD*=1.44 (low risk).

Hypothesis 1d suggested that people would be more likely to indicate an intention to Search For Information About Privacy on the website in the high risk group. This hypothesis was not supported, F (1,284) = 1.933, p =.166, η2 =.01. M=3.54, *SD*=1.57 (high risk), M=3.80, *SD*=1.73 (low risk).

Hypothesis 1e suggested that the Search For Information In General on the website, information about refund policies and information about how to order on the site would be higher in the high risk group. This hypothesis was not supported for the intent to search for information about refunds, F(1,284) = .019, p=.89, η2=.00 . M=5.31, *SD*= 1.53 (high risk), M=5.34, *SD*=1.66 (low risk). The hypothesis was also not supported for the intent to search for information about ordering off the site F(1,284) = .084, p=.773, η2=.00. M=4.62, *SD*=1.81 (high risk), M=4.58, *SD*=1.87 (low risk).

Hypothesis 1f suggested that those in the high risk condition would indicate a greater desire to search for information to protect their Future Privacy. This hypothesis was not supported. There was a marginally significant main effect of risk level on "search for information to protect privacy," F(1, 283) = 3.619, p = .058, η2=.01. The higher the risk, the less people indicated their intent to search for information about their privacy (M=4.52, *SD*=1.43) and the lower the risk the more likely they were to search for information about their privacy (M=4.82, *SD*=1.44).

Main effects of brand familiarity

Hypothesis 2a suggested that high brand familiarity would reduce perception of Online Privacy Risk. This hypothesis was not supported. The main effect of brand familiarity was non-significant F(1, 283) = 1.92, p =.167. η2 = .006. M=5.48, *SD*=.98 (high brand familiarity), M=5.27, *SD*=1.11(low brand familiarity).

Hypothesis 2b suggested there would higher Desire For Regulation of online privacy in the low brand familiarity group. This hypothesis was not supported. The main effect of brand familiarity was non-significant. F (1,283) =.110, p=.741, $\eta 2$ = .00. M=5.71, *SD*=1.03 (high brand familiarity), M=5.67, *SD*=.092 (low brand familiarity).

Hypothesis 2c suggested that people would feel less Control Over their Data online in the high brand familiarity group than in the low brand familiarity group. This hypothesis was not supported F (1, 284) = .001, p=.982, $\eta 2$ =.00. M=4.64, *SD*=1.49 (high brand familiarity), M=4.64, *SD*=1.49 (low brand familiarity).

Hypothesis 2d suggested high brand familiarity would have decrease the intention to Search For Information About Privacy on the website. This hypothesis was supported, F (1, 283) = 8.49, p <.05, $\eta 2$ =.03. Those in the familiar brand condition were less likely to seek information about privacy on the website than those in the unfamiliar brand condition, M=3.39, *SD*=1.75, M=3.96, *SD*=1.49, respectively.

Hypothesis 2e suggested high brand familiarity would decrease the indicated desire to Search For Information On The Website In General: search for refund and exchange information "refund" and search for information about how to place and order "ordering". This hypothesis was supported for the search for information about refunds factor, F(1, 283) = 4.29, p <.05, $\eta 2$ = .02. People within the familiar brand group were less likely to indicate that they were interested in additional information about how to make exchanges and what the policy was on refunds, M=5.13, *SD*=1.70 (high familiarity), M=5.52, *SD*=1.45(low familiarity). The hypothesis was also supported for the search for information about how to order, F(1, 284) = 11.01, p <.001, $\eta 2$=.04. In the familiar brand condition, people were less likely to indicate the desire to search for

information about ordering products from the site M=4.26, *SD*= 1.96 (high familiarity) versus the low familiarity group, M=4.97, *SD*=1.63.

Hypothesis 2f suggested brand familiarity would reduce the indicated desire to search for information to protect their Future Privacy where those in the low brand familiarity condition would search for more information on the topic. This hypothesis was not supported. There was a non-significant effect for level of brand familiarity on search for information privacy, $F(1, 283) = .029$, $p=.864$, $\eta 2= .00$. M=4.64, *SD*=1.50 (high brand familiarity), M=4.69, *SD*=1.39 (low brand familiarity).

Interaction effects

Hypothesis 3a suggested high brand familiarity would decrease perceived Online Privacy Risk in the high risk group. This hypothesis was not supported. The interaction was non-significant $F(1, 284) = .17$, $p =.681$, $\eta 2 = .00$.

Hypothesis 3b suggested high brand familiarity would decrease Desire For Regulation of online privacy in the high risk group. This hypothesis was not supported. The interaction was non-significant $F(1, 284) = .065$, $p =.799$, $\eta 2 =.00$.

Hypothesis 3c suggested high brand familiarity would increase perceived Control Over Their Data Online in the high risk group. This hypothesis was supported. The interaction was significant $F(1,284) = 4.211$, $p <.05$, $\eta 2 =.02$. It appears in the high risk condition brand familiarity interacts to lessen feelings of lower perceived control.

Hypothesis 3d suggested high brand familiarity would decrease intention to Search For Additional Information About Privacy on the website provided in the scenarios in the high risk group. This hypothesis was supported. This hypothesis was not supported. The interaction was non-significant $F(1,284) = 2.511$, $p=.114$, $\eta 2= .01$.

Hypothesis 3e suggested high brand familiarity would decrease intention to Search for Additional Information In General on the website provided in the scenarios in the high risk group was not supported. Neither interaction for either search for refund information or ordering information was significant $F(1, 284) = 1.99$, p=.159, $\eta 2 = .00$, $F(1, 283) = 1.30$, p=.263, $\eta 2 = .00$, respectively.

Hypothesis 3f suggested high brand familiarity would decrease intention to search for information to protect Future Privacy in the high risk group. This hypothesis was not supported. The interaction of brand familiarity level and risk level Future Privacy was non-significant, $F(1,283) = 1.694$ p=.194, $\eta 2 = .01$.

Regression Analyses

To test hypothesis 4a a hierarchical regression analysis was used to test the hypothesis. The hypothesis was supported. Interpersonal Trust significantly predicted perceived online privacy risk while controlling for demographics and the manipulations, R2 = .14, F(7, 278)=6.369, p<.001). The R squared change for the fourth model, (Interpersonal Trust was entered only in the fourth model through forced enter method) was .090, p<.001. Interpersonal trust significantly predicted perceived online privacy risk (β =-.302 , p<.001). Lower Interpersonal Trust is associated with higher perceived Online Privacy Risk. This interpretation is only true if the effects of the manipulation and demographics are held constant (See Table 4a).

To test hypothesis 4b, a hierarchical regression analysis was calculated to test the hypothesis. The hypothesis was supported. Interpersonal Trust significantly predicted Desire For Regulation while controlling for demographics and the manipulations, (R2 = .15, F(7, 278)=7.166, p<.001). The R squared change for the fourth model, (interpersonal

trust was entered only in the fourth model through forced enter method) was .083, p<.001. Interpersonal Trust was a significant predictor (β =-.290, p<.001). It was found that the risk manipulation was a marginally significant predictor of perceived online privacy risk (β = -.108, p=.057). Gender (β =.160, p<.05) and Age (β =.116, p<.05) were also significant predictors in this model. Lower interpersonal trust is associated with higher desire for regulation. This interpretation is only true if the effects of the manipulation and demographics are held constant (See Table 4b)

To test hypothesis 4c, a hierarchical regression analysis was calculated to test the hypothesis. The hypothesis was not supported. Interpersonal Trust did not significantly predict perceived Control Over Data while controlling for demographics and the manipulations and the model was not significant (F(7, 278)=1.638, p=.125) (See Table 4c).

To test hypothesis 4d, a hierarchical regression analysis was calculated to test the hypothesis. The hypothesis was not supported. Interpersonal Trust did not significantly predict intention to Search For Privacy Information on the websites provided in the scenarios while controlling for demographics and the manipulations, (R2 = .070, F(7, 278)=3.008, p<.05). The R squared change for the fourth model, (Interpersonal Trust was entered only in the fourth model through forced enter method) was .012, p=.063. Interpersonal Trust was not a significant predictor in the model (β =-.108, p=.063). It was found that brand familiarity was a significant predictor (β = -.183, p<.05). Gender (β =-.134, p<.05) was also a significant predictor in this model (See Table 4d).

To test hypothesis 4e, a series of hierarchical regression analyses was calculated to test the hypothesis. The hypothesis was not supported. Interpersonal Trust did not

significantly predict intention to search Information In General. Interpersonal Trust did not significantly predict refund information on the websites provided in the scenarios while controlling for demographics and the manipulations and the model was not significant, $F(7, 278)=1.347$, $p=.216$). Interpersonal Trust did not significantly predict intention to search for ordering information on the websites provided in the scenarios while controlling for demographics and the manipulations and the model was not significant, $F(7, 278)=1.347$, $p=.053$) (See Table 4e).

To test hypothesis 4f, a hierarchical regression analysis was calculated to test the hypothesis. The hypothesis was not supported. Interpersonal Trust did not significantly predict intention to search for Future Privacy while controlling for demographics and the manipulations and the model was not significant ($F(7, 278)=1.740$, $p=.10$).

To test hypothesis 5a, a hierarchical regression analysis was used to test the hypothesis. The hypothesis was supported. Institutional trust significantly predicted perceived Online Privacy Risk while controlling for demographics, the manipulations and interpersonal trust, $R2 = .19$, $F(8, 277)=8.142$, $p<.001$). The R squared change for the final model, (Institutional Trust was entered only in the final model in the last block through forced enter method) was .052, $p<.001$. Institutional Trust was a significant predictor ($\beta = -.239$, $p<.001$). Lower institutional trust is associated with a higher perceived online privacy risk. This interpretation is only true if the effects of the manipulation, demographics and Interpersonal Trust are held constant. Age was also a significant predictor in this model ($\beta = .137$, $p<.05$) (See Table 5a).

To test hypothesis 5b, a hierarchical regression analysis was used to test the hypothesis. The hypothesis was not supported. Institutional Trust did not significantly

predict perceived desire for additional regulation while controlling for demographics, the manipulations and Interpersonal Trust (R2 = .16, F(8, 277)=6.550, p<.001); (β = -.083, p=.153). However, in this model, Gender (β = .156, p <.05) and Age (β = .115, p<.05) were significant predictors). Risk was a marginally significant predictor (β = -.110, p =.052). (See Table 5b).

To test hypothesis 5c, a hierarchical regression analysis was used to test the hypothesis. The hypothesis was supported. Institutional Trust significantly predicted perceived control over data online while controlling for demographics, the manipulations and Interpersonal Trust, R2 = .073, F(8, 277)=2.730, p<.05). The R squared change for the final model, (Institutional Trust was entered only in the final model in the last block through forced enter method) was .033, p<.05. Institutional Trust was a significant predictor (β = .191, p<.05). Higher Institutional Trust is associated with a higher perceived control over data online. This interpretation is only true if the effects of the manipulation, demographics and interpersonal trust are held constant (See Table 5c).

To test hypothesis 5d, a hierarchical regression analysis was used to test the hypothesis. The hypothesis was not supported. Institutional Trust did not significantly predict intention to search for privacy information controlling for demographics, the manipulations and Interpersonal Trust, R2 = .072, F(8, 277)=2.693, p<.05); (β = .044, p=.469). However, in model five, Interpersonal Trust remained significant (β = -.119, p<.05). Brand Familiarity was a significant predictor (β = -.178, p<.05) as was Gender (β = -.132, p <.05). (See Table 5d).

To test hypothesis 5e, a series of hierarchical regression analyses were calculated. The hypothesis was not supported. Institutional Trust did not significantly predict

intention to search for refund information on the websites provided in the scenarios while controlling for demographics, the manipulations, and Interpersonal Trust and the model was not significant, $F(8, 277)=1.258$, $p=.265$). Institutional Trust did significantly predict intention to search for additional information about ordering information on the websites provided in the scenarios while controlling for demographics, the manipulations, and Interpersonal Trust $R2= .035$, $F(8, 278)=2.291$, $p<.05$); $\beta = .122$, $p <.05$. Higher Institutional Trust is associated with a higher desire to search for information about ordering products. Brand Familiarity was also a significant predictor ($\beta = -.191$, $p <.001$). This finding makes sense in the ordering and refund mechanisms where all consumers care about is how fast the product will arrive and if they can return the product. Trust in institutions may paradoxically lead them to search for more information in this arena because while they trust the institutions, order information is motivationally relevant at the time and encourages systematic processing despite heuristic cues, however, it appears that Brand Familiarity is still an important predictor for ordering behavior from a theoretical standpoint (See Table 5e).

To test hypothesis 5f, a hierarchical regression analysis was calculated to test the hypothesis. The hypothesis was not supported. Institutional Trust did not significantly predict intention to search for Future Privacy in the scenarios while controlling for demographics, the manipulations, and Interpersonal Trust and the model was not significant ($F(8, 277)=1.528$, $p=.147$).

6. DISCUSSION AND CONCLUSION

"Reason, is and ought only to be the slave of the passions, and can never pretend to any other office than to serve and obey them" – Thomas Hume

This study was based on the idea that people are not approaching the issue of online data privacy, exerting control over that data, giving meaningful consent to the use of their data in a deliberate, systematic way. Amid cries from consumer advocates, privacy researchers and the Edward Snowden leaks, a white paper was released in May of 2014 by the White House after an extensive look into the ways data online were being used and aggregated for both national security purposes, other issues of national concern, and for advertising and marketing purposes. The latter drew the most concern from the report, as the potential for discrimination based on inferred identification and the potential loss of personhood or "free will" as one becomes what they click as far as advertisements they see and potentially price ranges they receive in offers (Podesta, Pritzker, Moniz, Holdren, and Zients 2014). Dressed ominously in the popular press in on-going series like the *Wall Street Journal's* "What They Know" series, the title alone suggesting that "what they know" is more than the average person would like others to know and addressed by research entitled "American's Reject Tailored Advertising and Three Activities That Enable It" (Turow et. al. 2009), it would seem that consumers would be concerned about the process of surfing and shopping online. And it would seem from the aforementioned studies that people disliked relevant versus irrelevant ads. Joseph Turow would later in *The New York Times* while talking about Facebook privacy issues (outside the scope of this paper) say that everyone wanted relevant versus irrelevant advertisements (Goel 2014).

Previous studies suggest that when asked, people will say that they desire extra privacy protection and are concerned about their privacy online (Norber, Horne and Horne 2007; LaRose 2004). However, their behaviors belie their stated concerns and intentions as e-commerce continues to grow and advertisers gear up to increase the use of aggregated consumer data to serve more relevant advertisements to their audiences. The mismatch between the stated concerns and actual behaviors has been labeled the "privacy paradox" (Norberg, Horne and Horne 2007; Yap, Beverland and Bove 2009). Some suggest that a knowledge of the processes behind online behavioral advertising would both lessen concern and decrease feelings of risk. However, two studies, one conducted in the United States where an opt-out system is employed (Shoenberger and Thorson 2014) and one conducted in Europe where an opt-in system is employed (Smit et. al. 2014) found no correlation between actual knowledge of the processes of how data are used in OBA and perceptions of online privacy risk. Those studies culminated to this one. There are still many people who likely operate blindly online and are unaware of how their clickstream data are used. However, there are many others who are aware of at least the basics, and do nothing to protect themselves (whether that is deciding to not opt-in to receive relevant advertising or to opt-out of receiving relevant advertising) and yet, all of the above voice concern about their privacy online.

This study meant to tackle this unusual phenomenon, theorizing that people use heuristics to guide their behaviors online in everyday situations and when asked about their privacy, almost always opt for more privacy as that is what society deems as an acceptable stance (Haidt 2012). If informed consent is the goal, and it seems it should be if the predictions of a personhood being created, sold and then used to sell to the person

who created it, then how can a person be nudged into searching for and systematically or carefully considering options for their data collection online? And are brand familiarity and more contextually, in the United States, interpersonal and institutional trust important heuristics in lieu of the desired deliberate processing of data exchanges online? The following discussion of results may help to illuminate some of this complex issue.

Discussion of Findings and Implications for Theory, And Regulatory Action in the Realm of Consumer Data Used For Online Behavioral Advertising Purposes

The following sections review the findings reported in the previous chapter, examining the implications for consumer behavior in the online behavioral advertising context (online surfing, clicking and shopping) through the lens of HSM. Findings will be discussed and arranged by hypothesis and finally, a discussion of implications for future regulation of online data collection and aggregation will be discussed.

An overarching theme for the use of risk as a manipulation was that the high risk group behaved in an unusual, almost learned helplessness way. These findings, though, at first glance seem counterintuitive may point to a phenomenon found in the health communication literature. Turner and colleagues noted that even with topics more salient to the individual, such as health concerns and risks, not all people behave as though they may be at risk or search out information, perhaps because thinking about the risk causes anxiety and is distressing (2006). As a result, those in the high risk groups may have simply decided their ability to search for information to protect privacy or protect themselves in the future was out of their control and answered as such. It may have led them to exert a self-protective measure of indicating less online privacy risk and less desire for additional regulations to protect privacy in the future.

Additionally, it is possible that the high risk condition was too severe and caused an avoidance reaction which would account for lower desire to search for information to protect oneself in the future, lower perception of privacy risk online and less desire for additional regulation. A message about how to protect oneself was noted in the high risk message as suggested by those studying health risks in an effort to provide feelings of self-efficacy and reduce anxiety but the nature of online behavioral data collection is complex and a simple message to check privacy information may not have been enough to reduce the anxiety our participants felt when they received the high risk message. On the other hand, those in the low risk groups may have felt empowered by their status and encouraged, then, to indicate a greater perceived online privacy risk and desire additional regulation, keeping in line with the social desirability bias.

Brand familiarity, for the most part, fulfilled its role as a heuristic. For the questions asked immediately following each scenario, the pattern was the same. Brand familiarity always predicted less information search for ordering information, refund information or information about the privacy terms on the website in the scenario. This series of findings alluded to an important issue, namely what Rifon and colleague suggested in their discussion that "shopping concerns may be more salient than privacy concerns" (2005, p. 358). Certainly, amongst our participants, the more technical items such as ordering information and refunds were important, regardless of risk and searching for information about such concerns was driven solely by brand familiarity. When faced with an unfamiliar brand people want to know about issues relevant to their purchase; when will it arrive, and can I return it?

Only one of the hypothesized interactions was significant. When it came to perceived control over ones' data, the high risk condition interacted with the brand familiarity condition to mitigate feelings of lower perceived control. Again, it seems brand familiarity as a heuristic was useful in helping consumers navigate the online economy and offered a greater sense of control in the familiar condition even when a participant was in the high risk condition.

In an effort to add context to the discussion of online privacy and consumer behavior, especially in light of the privacy paradox, the results for hypotheses 4-5 were useful in getting one step further to the privacy paradox and a plausible explanation. Lower interpersonal trust was associated with higher perceived online privacy risk and desire for additional regulation. This finding made sense in light of the theory that interpersonal trust could be an overarching heuristic even when controlling for brand familiarity. When people trust each other, they tend to trust in the regulations as they stand and tend to trust that their data will not end up in the hands of criminals. Higher interpersonal trust was not associated with higher perceived control over data online but higher institutional trust did predict higher perceived control. This may be because while someone may trust another person, they do not trust them to control their data or have the ability to do so. However, consumers may trust in institutions to keep their data secure and safe and thus when trust in those institutions is high, so too is perceived control over data online.

Institutional and interpersonal trust were not significant predictors of future privacy search, searching for privacy on the scenario websites or searching the scenario websites for information about refunds. However, while not hypothesized, on searching

for information about privacy on the scenario websites was predicted by brand familiarity. This heuristic was integral in the decision-making of how much privacy information to search for while on the scenario's website where low brand familiarity led to higher desire to search for information. This alludes to the idea that in scenarios that are personally relevant, when a consumer is actually shopping and surfing online, brand familiarity is the main heuristic. Brand familiarity also predicted the desire to search for ordering information. In that case, high institutional trust also led to additional search. This finding was reconciled in the ordering and refund mechanisms where all consumers care about is how fast the product will arrive and if they can return the product. Trust in institutions may paradoxically lead them to search for more information in this arena because while they trust the institutions, order information is motivationally relevant at the time and encourages systematic processing despite heuristic cues, however, it appears that Brand Familiarity is still an important predictor for ordering behavior from a theoretical standpoint

People tend to say they feel high privacy risk when asked and it was assumed they would also ask for additional regulations regardless of condition. Both of the means were relatively high across the conditions on a 1-7 scale: desire for regulation, M=5.69, Median = 5.90, *SD*= 1.17, and perceived online privacy risk M=5.40, Median =5.50, *SD*= 1.03. Even though it seems that most people perceived online privacy risk and indicated a desire for additional regulation, institutional trust still predicted that those with high institutional trust desired less regulation and had less perceived privacy risk than those with lower institutional trust. This is an important finding, lending support to the theory that people lean on institutional trust as a heuristic in the online economy even

when answering questions in ways they believe are socially appropriate, thus the essence of the privacy paradox.

These findings taken together are of theoretical importance because they offer evidence about how consumers operate online. They do not appear to be consciously weighing pros and cons of website policies. In fact, even in the face of high risk for their data being used in ways they find inappropriate (high risk condition), only brand familiarity, operating as a heuristic, drove the decision whether to seek additional information about a website or not. Institutional trust was able to predict above and beyond the manipulations both perceived online privacy risk and desire for additional regulation, two variables thought to be linked to the privacy paradox. Their high means across conditions suggested the privacy paradox was at work via social desirability bias and institutional trust was able lessen even that paradox, predicting both desire for additional regulation and online privacy risk.

Discussion of Direction For Future Regulations

The idea that consumers take the time from their information soaked days to process privacy policies or information that would allow them to control their data online is a essentially a fiction. If the crux of the online behavioral advertising debate is actually about consumer privacy concern and consumer willingness to exert control over personal/clickstream data via an opt-out system, that goal is likely to fail.

The White House recently published a paper broadly exploring online data collection and the analyses of that data (Podesta et. al. 2014). The study encompassed not only the technologies used by the intelligence community but also those employed by industry. Especially concerning to the advertising industry was the report's focus on

"learning algorithms" used to serve online advertisements to consumers based on their online browsing activities and to predict purchase behaviors. The report noted that these algorithms could be used not just to serve relevant advertisements but also to discriminate based on inferences destined to error created by the aggregation and analyses of consumer data (Sanger and Lohr 2014).

The White House recommendations included (among others): increase transparency about how consumer data is used (especially in the realm of third party advertising, and tools that allow consumers to opt-out of online tracking should be strengthened (Podesta et. al. 2014). This study suggests that new ideas be proliferated as increased transparency has usually meant privacy seals and even the most knowledgeable consumers fall victim to the false security of a safety seal, not looking to read its contents or find out what kinds of safety it promises (Rifon, LaRose, Choi 2005). The issue with opt-out and opt-in systems were nearly addressed by Podesta himself as he noted that consumers click on terms of service nearly all the time without reading them and pondered whether such a process sill gave consumers the control to protect the privacy of their data online (Podesta, et. al. 2014). To continue to pressure industry to follow either of the aforementioned paths would do a disservice to both the industry and consumers.

The fact that consumers tend to ignore privacy icons or information about how to protect their information online and continue to act in ways that are counter to self-protection even in the face of a serious warning that their personal data is at risk of being used in ways they will find inappropriate is a blow to the notion that consumers desire to exercise control over their data online. It may be that consumers are not as interested in

exercising control but instead desire the ability to trust their data is being used in ways they deem appropriate and have remedies to address perceived mishandling of data.

Trust in the institutions supporting data collection such as the advertising industry and the government have likely led to the success of such collection with minimal outcry from consumers/citizens because consumers/citizens believe, in large part, that their data will be kept secure by responsible institutions. Accountability to consumers/citizens when data are mishandled or handled in ways in which they can reasonably disapprove must be outlined and upheld.

Those housing and analyzing the voluminous amounts of consumer data should work within an ethical framework and take care to be transparent in the collection and use of the data to consumers and maintain the integrity and safety of the data or risk instances of mishandling and data breaches. Data breaches and leaks of consumer data may eventually result in the erosion of public trust in institutions such as the advertising industry and the government. Remedies must be woven into regulations for those injured by data breaches. Public trust in such institutions is integral to an efficiently functioning society (Freitag & Buhlmann , 2009).

The ability to correct information that is false or inferences derived from imperfect analysis must be easy for the consumer. The ability to correct false information is entwined with the notion of institutional trust but also touches on fairness. If information being collected about a consumers' online activities are in any way attached to personally identifiable information, something it should not be but inferences from complex analyses of large amounts of data may come dangerously close to linking

the consumer to her searches, she should have the ability to correct that information in the aggregator database.

Through the vast amount of data collected on consumers as they surf online, it is possible that inferences could be made that nearly identify the person surfing online and despite the lack of personally identifiable information (e.g., social security numbers). It would be possible then for a company to use information to predict those who would not show up to work or those with certain illnesses and discriminate based on such predictions. Safeguards must be in place to prevent those who would discriminate based on inferences made from big data statistics which always comes with a percentage of error.

The effort and expense put into designing and promoting privacy seals (e.g., the Trust-E icon) that can be placed like badges on a website are meant to offer transparency and comply with the Federal Trade Commissions' insistence on notice and choice in the realm of online data collection. The opt-out system in the United States currently requires a consumer to click on the privacy seal or icon and read the instructions for ways to opt-out of online tracking used to serve relevant advertisements and predict buying behaviors. The efforts concentrating on a seal, alone, may be misguided.

Consumers must be given reasonable notice of personal data collection and use and the ability to make informed decisions on whether to opt out of data collection. Due to the lack of consumer attention paid to privacy seals, further research in this area is needed. Either privacy notices that catch the consumer's attention and motivate them to fully understand the contents must be created or those using a privacy policy should abide

by regulations guaranteeing an agreed upon set of rules for data security, and permissible uses (Turow et.al., 2008).

This set of regulations would also benefit from empirical research belying the important elements of privacy in regards to online data and perhaps, because not all data is equal in terms of sensitivity, a taxonomy of the types of data consumers would like to have control over. Gamefication of privacy seals may be an interactive way to assure informed consent to data use and make a normally boorish boilerplate privacy seal or information more likely to be attended to.

Limitations

This study suffered from limitations. One being the potential over aggressiveness of the high risk message. Instead of eliciting an information search behavior, it appears the message may have elicited an avoidance and self-protective type behavior.

Conclusion

This study meant to attempt to understand the way in which consumers navigate the online economy, in the narrow context of clickstream data collection and shopping online. As theorized, it appears that consumers are using heuristics such as brand familiarity and institutional trust to guide their decisions of how much information they will look for and understand on a website before making a purchase. A familiar brand leads to significantly less indication to search than an unknown brand leading to the conclusion that brand familiarity is a heuristic employed in this situation.

The privacy issue stems from the assumption that the information collected and aggregated is, in some ways, regarded by the consumer as private. However, this may not be the case. The aggregation of information about a consumer could in the near future,

perhaps depriving the consumer of the ability to define themselves online. People who study this issue make the assumption for consumers that they would be wiser to keep this information within their control at the very least, but if they decide to exert no control, as we have seen for the majority of our sample, then that is a valid choice, as well.

When the choice hinges on control over data, social contract theory offers useful guidance asserting that a contract between a consumer and a business/advertiser is breached if the data is collected and/or used in a fraudulent way. The existence of consumer privacy on the Internet is derived from control exerted over the data they release (Milne and Gordon 1993). Social contract theory also posits that consumers will actively seek out information, carefully examining privacy policies before committing to a relationship with a business (Milne and Gordon 1993). We know the latter part of the equation, for the most part, does not happen. Further evidence that privacy policies affect behavior, influencing consumer decisions on whether or not to trust a site, interestingly regardless of the length/content of the policy, add further support to the theory that consumers navigate the online environment using a heuristics and rarely, if ever, seek ways to control their data or salvage any piece of privacy they may lay claim to online (Milne and Gorndon 1993; Miyazaki and Fernandez 2000).

The trust that data are safe and transactions online are safe will persist until there are serious consequences that ignite the passions of the consumer. Until then, they will save more effortful processing for things more motivationally relevant to them.

7. TABLES

TABLE 1

Measurement Scales Used in the Study

Scale	Scale items	α, r
Institutional Trust (adapted from Siegrist, 2000)	How much do you trust the following institutions or persons in terms of how well they fulfill their responsibilities in collecting and handling consumer data collected online… 1. The government 2. Individual advertisers 3. The advertising industry 4. Individual brands	0.772
Interpersonal Trust (adapted from: Das, 2003)	Please indicate your level of agreement… 1. It is safe to believe that in spite of what people say. 2. In dealing with strangers one is better off to be cautious until they have provided evidence that they are trustworthy. 3. If you are not careful, others can easily manipulate you. 4. Most repairmen will not overcharge even if they think you are ignorant of their specialty (flipped).	0.753
Perceived Online Privacy Risk (Shoenberger & Thorson, 2014)	Please indicate your level of agreement with the following… 1. Data used to serve relevant advertising may be compromised. 2. Data companies collect about me could end up in the hands of criminals. 3. Data companies collect about me might be used in ways that make me feel uncomfortable. 4. One my data is collected, I have no control over how it is used	0.827
Perceived Control Over Data Online (lower scores indicate lower perception of control)	Please indicate your level of agreement with the following… 1. I feel that I have control over my data online. 2. I believe I can opt-out of allowing advertisers and companies to collect my online behavioral data (ie. remembering what sites I visit, remembering what I click on in those sites to serve advertising that they believe will be more relevant to me). 3. I can use online privacy tools to remain anonymous online. 4. I understand how my online behavioral data is used online	0.766

Table 1, cont.

Scale	Scale items	α, r
Desire for Regulation (adapted from concerns espoused in (Podesta, Pritzker, Moniz, Holdren, and Zients, 2014)	Please indicate your level of agreement with the following… 1. Regulators should do more to protect my data online. 2. I am concerned about my privacy online. 3. I would like to know what safeguards are in place in the event of a data breach 4. I would like to know how I may be compensated in the event of a data breach. 5. I would like to know what companies are doing to keep my personal data secure. 6. I would like to know what the federal government is doing to keep my personal data secure. 7. I would like to see additional regulation enacted to protect my data privacy online. 8. I would like a new law enacted to protect my data online.	0.933
Privacy Search (symptom of systematic processing) (created from items on actual Bestbuy.com and Walmart.com websites)	The following information is on X's website. Please indicate how likely you would be to seek out and read about the following pieces of information before clicking through the website and choosing your new camera/bike?... 1. How secure the website is. 2. Information the website collect about you. 3. Use of cookies on the website. 4. How the site uses pattern recognition to link your purchase history to products you might like 5. Information the site exchanges with third party advertisers. 6. How the site uses your credit card information. 7. How to opt-out of the site's cookie tracking system. 8. How the site ensures consumer data privacy. 9. The website's mobile application privacy options. 10. Contact information in case you have privacy related questions. 11. A pledge of accountability by the company. 12. How your IP address and other information are collected by social media widgets on the site (for example, Facebook or Pinterest icon).	0.982

Table 1, cont.

Scale	Scale items	α, r
Refund Search (symptom of systematic processing) (created from items on actual Bestbuy.com and Walmart.com websites)	The following information is on X's website. Please indicate how likely you would be to seek out and read about the following pieces of information before clicking through the website and choosing your new camera/bike?... 1. Defective items. 2. Exchanges. 3. Refunds. 4. Return exceptions.	r = .711
Ordering Search (symptom of systematic processing) (created from items on actual Bestbuy.com and Walmart.com websites)	The following information is on X's website. Please indicate how likely you would be to seek out and read about the following pieces of information before clicking through the website and choosing your new camera/bike?... 1. How to place your order. 2. Payment Options.	0.912
Future Privacy (adapted from Turow and Hennessey, 2007)	Please indicate how likely you would be to do the following before clicking through a website in the future… 1. Choose not to register with a site because it asks for too much personal information. 2. Search for instructions about how to protect yourself on the web.	r = .662

TABLE 2

Intercorrelations Among Variables

Measure	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. Gender	___														
2. Age	.106	___													
3. Education	.004	.079	___												
4. Income	-.010	.034	.254**	___											
5. Desire for regulation	.189**	.144**	.038	.021	___										
6. Perceived Risk	.082	.159**	.035	.029	.458**	___									
7. Risk (High/Low)	-.079	-.108	-.005	.142*	-.154**	-128*	___								
8. Brand Familiarity	-.121*	.095	-.065	-.041	.015	.075	.024	___							
9. Institutional Trust	-.034	-.025	-.086	-.003	-.161**	-.309**	-.004	-.107	___						
10. Interpersonal Trust	.044	.027	.056	.017	-.300**	-.300**	.084	.020	.243**	___					
11. Control Over Data	-.047	-.090	-.129*	-.003	-.046	-.099	-.087	-.004	.204**	.036	___				
12. Ordering Search	-.011	-.025	-.022	-.017	.200**	.063	.012	-.193**	.119*	-.071	.092	___			
13. Refund Search	-.032	.016	.035	.042	.247**	.109	-.009	-.121*	-.055	-.116*	.133*	.421**	___		
14. Privacy Search	-.105	-.068	-.041	-.062	-.295**	.017	-.078	-.170**	.042	-.116.	.355**	.472**	.507**	__	
15. Future Privacy	.015	.057	.031	.020	.474**	.271**	-.105	-.017	-.026	-.170**	.262**	.287**	.350**	.647**	__

** Correlation is significant at the .01 level (2-tailed)

*Correlation is significant at the .05 level (2-tailed)

TABLE 3

Summary of Anova Results

Factor/DV	Risk Main Effect	Brand Familiarity Main Effect	Interaction
Perceived online privacy risk	Yes, but means are lower in the high risk group. HR *M = 5.29*, LR *M = 5.52* F(1,283) = 5.27, p < .05.	no	no
Desire for Regulation	Yes but again: High risk had lower M for high risk group. HR *M = 5.51*, LR *M = 5.87* F(1,283) = 7.20, p < .05.	no	no
Perceived control over data	Marginal, p = .12 high risk M = 4.52, Low risk: 4.82: This makes sense because in high risk you perceive less control over your data. F(1, 283) = 2.50, p = .115	no	Yes. It appears in the high risk condition brand familiarity interacts to lessen feels of lower perceived control F(1,284) = 4.21, P < .05.
Privacy search	no	Yes, familiar brand condition were less likely to seek information about privacy on the website than those in the unfamiliar brand condition. F(1, 283) = 8.49, p < .05 M = 3.39, *SD* = 1.75 (familiar) M = 3.96, *SD* = 1.49 (unfamiliar)	no

Table 3, cont.			
Factor/DV	Risk Main Effect	Brand Familiarity Main Effect	Interaction
Refund search	no	Yes, people in the familiar brand group were less likely to indicate they would search for information about making refunds and exchanges. $F(1, 283) = 4.29$, $p < .05$ $M = 5.13$, $SD = 1.70$ (familiar) $M = 5.52$, $SD = 1.45$ (unfamiliar)	no
Ordering search	no	Yes, people in the familiar brand group were less likely to indicate they would search for information about how to order from the website in the scenario. $F(1, 283) = 11.01$, $p < .001$ $M = 4.26$, $SD = 1.96$ (familiar) $M = 4.97$, $SD = 1.63$ (unfamiliar)	no
Future Privacy	Marginal and in the wrong direction. $F(1, 283) = 3.62$, $p = .058$ $M = 4.52$, $SD = 1.43$ (High Risk) $M = 4.82$, $SD = 1.44$ (Low Risk)	no	no

ANOVAs by Dependent Variable

Table 4a

Online Privacy Risk

	df	F	η2	p
Risk	1	5.27	.02	.02
Brand Familiarity	1	1.92	.01	.17
Risk x Brand Familairty	1	.17	.00	.68

*significant at p < .05

Table 4b

Desire for Regulation

	df	F	η2	p
Risk	1	7.20	.02	.01
Brand Familiarity	1	.11	.00	.74
Risk x Brand Familairty	1	.07	.00	.80

*significant at p < .05

Table 4c

Perceived Control Over Data

	df	F	η2	p
Risk	1	2.50	.01	.12
Brand Familiarity	1	.001	.00	.98
Risk x Brand Familairty	1	4.50	.02	.04

*significant at p < .05

Table 4c

Intention to Search for Privacy Information on Website

	df	F	η2	p
Risk	1	1.93	.01	.17
Brand Familiarity	1	8.49	.03	.00
Risk x Brand Familairty	1	4.21	.01	.19

*significant at p < .05

Table 4e (Refund Search)

Intention to Search for General Information on Website (Refund)

	df	F	η2	p
Risk	1	.02	.00	.89
Brand Familiarity	1	4.29	.02	.04
Risk x Brand Familairty	1	1.99	.01	.16

*significant at p < .05

Table 4e (Ordering Search)

Intention to Search for General Information on Website (Ordering)

	df	F	η2	p
Risk	1	.084	.00	.77
Brand Familiarity	1	11.01	.04	.00
Risk x Brand Familiarity	1	1.30	.00	.26

*significant at p < .05

Table 4f

Intention to Search for Information to Protect Privacy in the Future

	df	F	η2	p
Risk	1	3.62	.01	.06
Brand Familiarity	1	.03	.00	.86
Risk x Brand Familiarity	1	1.69	.01	.19

*significant at p < .05

Table 5

Table 5a: Predictors of Perceived Online Privacy Risk

		b	SE B	β	*p*
Step 1					
	Constant	4.643	.325		.000
	Gender	.137	.122	.066	.262
	Age	.013	.005	.150	.012
	Education	.017	.057	.018	.769
	HHI	.013	.039	.020	.740
				R2 = .030	
Step 2					
	Constant	4.541	.335		.000
	Gender	.156	.123	.076	.204
	Age	.012	.005	.141	.018
	Education	.021	.057	.023	.709
	HHI	.014	.039	.022	.715
	Brand Familiarity	.149	.123	.072	.227
				R2 = .035	
Step 3					
	Constant	4.692	.342		.000
	Gender	.141	.123	.068	.252
	Age	.011	.005	.129	.032
	Education	.018	.057	.019	.753
	HHI	.025	.039	.040	.515
	Brand Familiarity	.157	.123	.076	.201
	Risk (Low/High)	-.238	.123	-.115	.054
				R2 = .048	
Step 4	Constant	5.444	.355		.000
	Gender	.117	.117	.057	.318
	Age	.012	.005	.140	.015
	Education	.034	.054	.036	.534
	HHI	.023	.037	.037	.528
	Brand Familiarity	.164	.117	.080	.161
	Risk (Low/High)	-.183	.118	-.089	.120
	Interpersonal Trust	-.297	.055	-.302	.000
				R2 = .116	
Step 5	Constant	6.227	.391		.000
	Gender	.098	.114	.048	.343
	Age	.012	.005	.137	.025
	Education	.009	.053	.009	.858
	HHI	.027	.036	.042	.437
	Brand Familiarity	.104	.114	.051	.479
	Risk (Low/High)	-.198	.114	-.096	.040
	Interpersonal Trust	-.238	.055	-.242	.000
	Institutional Trust	-.411	.097	-.239	.000
				R2 = .190	

Note: *R2* = .05 for step 3; Δ *R2* = .090 for step 4 ($p < .001$); *R2* = .14 for step 4; Δ *R2* = .052 for step 5 ($p < .001$)

Table 5b: Predictors of Desire for Regulation

		b	SE B	β	*p*
Step 1					
	Constant	4.535	.364		.000
	Gender	.412	.137	.176	.003
	Age	.012	.006	.123	.037
	Education	.025	.064	.024	.694
	HHI	.009	.043	.013	.834
				R2 = .052	
Step 2					
	Constant	4.493	.376		.000
	Gender	.420	.138	.179	.003
	Age	.012	.006	.120	.043
	Education	.027	.064	.026	.673
	HHI	.010	.043	.013	.825
	Brand Familiarity	.062	.138	.026	.656
				R2 = .053	
Step 3					
	Constant	4.690	.383		.000
	Gender	.399	.137	.171	.004
	Age	.010	.006	.105	.076
	Education	.023	.064	.021	.723
	HHI	.024	.044	.034	.577
	Brand Familiarity	.072	.137	.031	.598
	Risk (High/Low)	-.312	.138	-.133	.024
				R2 = .070	
Step 4					
	Constant	5.508	.399		.000
	Gender	.373	.131	.160	.005
	Age	.011	.005	.116	.041
	Education	.040	.061	.038	.513
	HHI	.022	.042	.031	.594
	Brand Familiarity	.080	.131	.034	.543
	Risk (High/Low)	-.252	.132	-.108	.057
	Interpersonal Trust	-.323	.062	-.290	.000
				R2 = .153	
Step 5					
	Constant	5.815	.452		.000
	Gender	.366	.131	.156	.006
	Age	.011	.005	.115	.042
	Education	.030	.061	.028	.624
	HHI	.024	.042	.033	.573
	Brand Familiarity	.057	.132	.024	.669
	Risk (High/Low)	-.258	.132	-.110	.052
	Interpersonal Trust	-.300	.064	-.269	.000
	Institutional Trust	-.161	.112	-.083	.153
				R2 = .159	

Note: *R2* = .070 for step 3; Δ *R2* = .083 for step 4 (p < .001); *R2* = .153 for step 4; Δ *R2* = .006 for step 5 (p is *NS*)

Table 5c: Predictors of Perceived Control Over Data Online

		b	SE B	β	*p*
Step 1					
	Constant	5.107	.361		.000
	Gender	-.088	.136	-.038	.518
	Age	-.007	.006	-.077	.199
	Education	-.136	.063	-.131	.033
	HHI	.023	.043	.033	.591
				R2 = .025	
Step 2					
	Constant	5.120	.373		.000
	Gender	-.090	.137	-.039	.511
	Age	-.007	.006	-.076	.208
	Education	-.137	.063	-.131	.033
	HHI	.023	.043	.033	.594
	Brand Familiarity	-.019	.137	-.008	.891
				R2 = .026	
Step 3					
	Constant	5.276	.382		.000
	Gender	-.106	.137	-.046	.437
	Age	-.008	.006	-.088	.146
	Education	-.140	.063	-.135	.028
	HHI	.035	.043	.049	.425
	Brand Familiarity	-.010	.137	-.004	.940
	Risk (High/Low)	-.248	.137	-.108	.072
				R2 = .037	
Step 4					
	Constant	5.128	.415		.000
	Gender	-.102	.137	-.044	.458
	Age	-.009	.006	-.090	.138
	Education	-.143	.064	-.138	.025
	HHI	.035	.044	.050	.420
	Brand Familiarity	-.012	.137	-.005	.932
	Risk (High/Low)	-.259	.138	-.113	.062
	Interpersonal Trust	.058	.065	.054	.366
				R2 = .040	
Step 5					
	Constant	4.433	.464		.000
	Gender	-.085	.135	-.037	.528
	Age	-.008	.006	-.087	.141
	Education	-.121	.063	-.116	.056
	HHI	.032	.043	.046	.452
	Brand Familiarity	.042	.136	.018	.760
	Risk (High/Low)	-.246	.136	-.107	.071
	Interpersonal Trust	.006	.066	.005	.930
	Institutional Trust	.365	.115	.191	.002
				R2 = .073	

Note: *R2* = .037 for step 3; Δ *R2* = .003 for step 4 (p is *NS*); *R2* = .040 for step 4; Δ *R2* = .033 for step 5 (p < .05)

Table 5d: Predictors of Privacy Search

		b	SE B	β	*p*
Step 1					
	Constant	4.737	.521		.000
	Gender	-.328	.196	-.099	.095
	Age	-.007	.008	-054	.396
	Education	-.033	.092	-.022	.715
	HHI	-.056	.062	-.055	.367
				R2 = .002	
Step 2					
	Constant	5.161	.530		.000
	Gender	-.410	.194	-.124	.036
	Age	-.004	.008	-.032	.586
	Education	-.052	.090	-.035	.567
	HHI	-.062	.061	-.061	.314
	Brand Familiarity	-.616	.195	-.187	.002
				R2 = .043	
Step 3					
	Constant	5.329	.543		.000
	Gender	-.427	.194	-.129	.029
	Age	-.006	.008	-.041	.490
	Education	-.056	.090	-.037	.536
	HHI	-.049	.062	-.048	.430
	Brand Familiarity	-.608	.194	-.184	.002
	Risk (High/Low)	-.270	.195	-.082	.168
				R2 = .043	
Step 4					
	Constant	5.763	.588		.000
	Gender	-.441	.194	-.134	.02
	Age	-.005	.008	-.037	.531
	Education	-.047	.090	-.031	.604
	HHI	-.050	.062	-.049	.417
	Brand Familiarity	-.603	.194	-.183	.002
	Risk (High/Low)	-.239	.195	-.073	.221
	Interpersonal Trust	-.170	.091	-.108	.063
				R2 = .048	
Step 5					
	Constant	5.533	.699		.000
	Gender	-.435	.194	-.132	.026
	Age	-.005	.008	-.037	.536
	Education	-.039	.091	-.026	.665
	HHI	-.051	.062	-.050	.409
	Brand Familiarity	-.586	.195	-.178	.003
	Risk (High/Low)	-.235	.195	-.071	.230
	Interpersonal Trust	-.280	.095	-.119	.048
	Institutional Trust	.120	.166	.044	.469
				R2 = .062	

Note: *R2* = .059 for step 3; Δ *R2* = .012 for step 4 (p is *NS*); *R2* = .070 for step 4; Δ *R2* = .002 for step 5 (p is *NS*)

Table 5e: Predictors of Ordering Search

		b	SE B	β	*p*
Step 1					
	Constant	4.706	.583		.000
	Gender	-.015	.220	-.014	.816
	Age	.004	.009	.029	.633
	Education	-.035	.103	-.021	.735
	HHI	-.015	.070	-.013	.831
				R2 = .002	
Step 2					
	Constant	5.228	.593		.000
	Gender	-.152	.218	-.041	.488
	Age	.008	.009	.052	.377
	Education	-.058	.101	-.034	.570
	HHI	-.022	.069	-.019	.751
	Brand Familiarity	-.758	.218	-.206	.001
				R2 = .043	
Step 3					
	Constant	5.175	.610		.000
	Gender	-.147	.218	-.040	.502
	Age	.008	.009	.055	.359
	Education	-.056	.101	-.034	.580
	HHI	-.026	.070	-.023	.710
	Brand Familiarity	-.761	.218	-.207	.001
	Risk (High/Low)	.085	.219	.023	.699
				R2 = .043	
Step 4					
	Constant	5.489	.663		.000
	Gender	-.157	.218	-.043	.473
	Age	.009	.009	.057	.337
	Education	-.050	.102	-.030	.626
	HHI	-.027	.069	-.023	.701
	Brand Familiarity	-.758	.218	-.206	.001
	Risk (High/Low)	.107	.220	.029	.626
	Interpersonal Trust	-.123	.103	.070	.233
				R2 = .048	
Step 5					
	Constant	4.775	.749		.000
	Gender	-.140	.217	-.038	.521
	Age	.009	.009	.059	.323
	Education	-.027	.102	-.016	.794
	HHI	-.030	.069	-.026	.669
	Brand Familiarity	-.703	.219	-.191	.001
	Risk (High/Low)	.121	.219	.033	.582
	Interpersonal Trust	-.177	.106	-.101	.095
	Institutional Trust	.375	.186	.122	.045
				R2 = .062	

Note: *R2* = .043 for step 3; Δ *R2* = .005 for step 4 (p is *NS*); *R2* = .048 for step 4; Δ *R2* = .014 for step 5 (p < .05)

Table 6: Summary of exploratory factor analysis results for the online data security items.

		Rotated Factor Loadings	
Item	Desire for Regulation	Perceived Online Privacy Risk	Control Over Data
I feel I have control over my data online.	-.076	-.218	**.678**
I believe I can opt-out of allowing advertisers and companies to collect my online behavioral data.	.026	-.132	**.673**
I can use online privacy tools to remain anonymous.	-.024	.047	**.688**
I understand how my online behavioral data is used online.	.006	.073	**.582**
Data used to serve relevant advertising may be compromised.	.181	**.744**	.047
Data companies collect about me could end up in the hands of criminals.	.216	**.752**	-.038
Data companies collect about me might be used in ways I find uncomfortable.	.242	**.751**	-.011
Once my data is collected, I have no control over how it is used.	.168	**.582**	-.209
I would like to see additional regulation enacted to protect my data online.	**.791**	.248	-.233
I would like a new law enacted to protect my data online.	**.816**	.157	-.254
Regulators should do more to protect my data online.	**.828**	.120	-.233
I am concerned about my privacy online.	**.630**	.352	-.102
I would like to know what safeguards are in place in the event of a data breach.	**.757**	.206	.204
I would like to know how I may be compensated in the event of a data breach.	**.735**	.213	.176
I would like to know what companies are doing to keep my personal data secure.	**.798**	.243	.151
I would like to know what the federal government is doing to keep my personal data secure.	**.838**	.078	.045
Eigenvalues	6.31	2.57	1.90
% of variance	39.50	16.03	11.81
α	.93	.83	.77

Table 7: Means and Standard Deviations by Condition for Perceived Control Over Data

Condition	N	M	STD
Low Risk Unfamiliar Brand	70	4.55	1.17
Low Risk Familiar Brand	71	4.27	1.15
High Risk Unfamiliar Brand	71	4.06	1.13
High Risk Familiar Brand	77	4.33	1.10

8. APPENDICES

Appendix A

Pre-test Questionnaire

You are invited to participate in a research project about preferences for online shopping. The purpose of this study is to find out if people shop online in different ways. Participants will be entered into a drawing for a chance to win $50. Participation in the study is voluntary and you must be 18 years of age to participate. Your name and responses to the questions will be completely anonymous. You may refuse to answer any questions with no penalty. The risk in participating is no greater than what would be expected in a daily conversation about similar topics. By emailing for the link to complete this experiment, you are agreeing to participate in the study. If you have any questions or concerns about this research project please contact Heather Shoenberger at hrskv9@mail.missouri.edu or Dr. Esther Thorson at thorsone@missouri.edu or the Campus IRB at 573-882-9585

Please tell us a little about yourself.

	Never	Rarely	Sometimes	Most of the Time	Always
Have your computer save passwords.	•	•	•	•	•
Read unsolicited e-mail.	•	•	•	•	•
Provide a false or fictitious name when registering on a website.	•	•	•	•	•
Use public wi-fi.	•	•	•	•	•
Log onto online accounts using public computers.	•	•	•	•	•
Have a virus checker installed on your computer.	•	•	•	•	•
Set up your browser to reject unnecessary cookies.	•	•	•	•	•
Lock your computer when it is not in use.	•	•	•	•	•
Upgrade your browser to the newest version.	•	•	•	•	•
Open an email without a subject.	•	•	•	•	•
Use a password that can be found in the dictionary.	•	•	•	•	•
Accept unknown "friends" on social networking sites.	•	•	•	•	•
Make sure online forms are secure before filling them out.	•	•	•	•	•

Clear computer's cache after browsing	•	•	•	•	•
Frequently scan your computer for spyware.	•	•	•	•	•
Use a separate email account that you use solely for the purpose of registering on websites.	•	•	•	•	•
Save your credit card information in an online store's database.	•	•	•	•	•
When you get an e-mail from a financial institution asking for information updates, you click the link and fill out their update form.	•	•	•	•	•
Look for and read privacy statements on the Web.	•	•	•	•	•
Use anonymizers while browsing the web.	•	•	•	•	•
Include biographical information about you online (e.g., on Facebook or other site).	•	•	•	•	•
Use social networking sites.	•	•	•	•	•
Post on social networking sites.	•	•	•	•	•

Please indicate your answer to the following questions.

	Never	Rarely	Sometimes	Most of the time	Always
How often do you encounter advertising based on what you have previously searched for?	•	•	•	•	•
How often do you click on advertisements that offer discounts for a product?	•	•	•	•	•

	0 hours	less than an hour	1-2 hours	2-3 hours	3-4 hours	4 or more hours
About how much time do you spend online each day?	●	●	●	●	●	●
About how much time do you spend on social networking sites each day?	●	●	●	●	●	●
About how much time do you spend shopping online each day?	●	●	●	●	●	●

How many purchases would you estimate you have made online in the past month?

- 0
- 1
- 2
- 3
- 4
- 5 or more

What is your gender?

- Male
- Female

What is your age?

Please indicate your highest level of education.

- some high school
- high school/GED
- some college
- college
- some graduate school
- graduate school

Please indicate your yearly household income

- Under 10,001
- 10,001-20,000
- 20,001-40,000
- 40,001-60,000
- 60,001- 80,000
- 80,001 - 100,000
- Over 100,001

Thank you! Please be patient while we calculate your personal online data risk quotient.

<<<Here participant saw a timer counting backwards for 10 seconds>>>

Randomly the participant was shown either a high risk or low risk message after the ten seconds had passed.

The second part of the study asks you to tell us a little bit more about your online purchasing habits. Please try to imagine yourself in the following online shopping scenarios.

SCENARIO 1:

Imagine you have decided to add biking to your fitness routine. You have decided to buy a bicycle that costs about $650 and that you believe is a good fit for your biking needs.

You have decided to purchase your new bicycle from Walmart.com OR SuppliesPlus.com.

The following information is available on the Walmart.com/SuppliesPlus.com website. Please indicate how likely you would be to seek out and read about the following pieces of information before clicking through the website and choosing your new bike.

	Very Unlikely	Unlikely	Undecided	Likely	Very Likely
How to place your order.	●	●	●	●	●
Payment options.	●	●	●	●	●
How secure the website is.	●	●	●	●	●
Fair Credit Billing Act.	●	●	●	●	●
Information the website collects about you.	●	●	●	●	●
Use of cookies on the website.	●	●	●	●	●
Rebates.	●	●	●	●	●
How the site uses pattern recognition to link your purchase history to products you might like.	●	●	●	●	●
Information the site exchanges with third party advertisers.	●	●	●	●	●
Defective items.	●	●	●	●	●
Exchanges.	●	●	●	●	●
Refunds.	●	●	●	●	●
Return exceptions.	●	●	●	●	●
How the site uses your credit card information.	●	●	●	●	●
Order processing time.	●	●	●	●	●
How to opt-out of the site's cookie tracking system.	●	●	●	●	●
How the site ensures consumer data privacy.	●	●	●	●	●

SCENARIO 2:

Imagine you are about to go on a once in a lifetime vacation. In preparation for this trip, you plan to buy a new camera to capture all of the important moments. You have decided to buy a camera that costs about $500 and that you believe meets all of your photography needs.

You have decided to purchase your new camera from BestBuy.com OR CamerasGalore.com.

The following information is available on the BestBuy.com (CamerasGalore.com) website. Please indicate how likely you would be to seek out and read about the following pieces of information clicking through the website and choosing your new camera.

	Very Unlikely	Unlikely	Undecided	Likely	Very Likely
How to place your order.	●	●	●	●	●
Payment options.	●	●	●	●	●
How secure the website is.	●	●	●	●	●
Fair Credit Billing Act.	●	●	●	●	●
Information the website collects about you.	●	●	●	●	●
Use of cookies on the website.	●	●	●	●	●
Rebates.	●	●	●	●	●
How the site uses pattern recognition to link your purchase history to products you might like.	●	●	●	●	●
Information the site exchanges with third party advertisers.	●	●	●	●	●
Defective items.	●	●	●	●	●
Exchanges.	●	●	●	●	●
Refunds.	●	●	●	●	●
Return exceptions.	●	●	●	●	●
How the site uses your credit card information.	●	●	●	●	●
Order processing time.	●	●	●	●	●
How to opt-out of the site's cookie tracking system.	●	●	●	●	●
How the site ensures consumer data privacy.	●	●	●	●	●

I feel that I have control over my data online.	•	•	•	•	•
I believe I can opt-out of allowing advertisers and companies to collect my online behavioral data (ie. remembering what sites I visit, remember what I click on in those sites to serve advertising that they believe will be more relevant to me).	•	•	•	•	•
I can use online privacy tools to remain anonymous online.	•	•	•	•	•
I understand how my online behavioral data is used online.	•	•	•	•	•
Data used to serve relevant advertising may be compromised.	•	•	•	•	•
Data companies collect about me could end up in the hands of criminals.	•	•	•	•	•
Data companies collect about me might be used in ways that make me feel uncomfortable.	•	•	•	•	•

Once my data is collected, I have no control over how it is used.	•	•	•	•	•
I would like to see additional regulation enacted to protect my data privacy online.	•	•	•	•	•
I would like a new law enacted to protect my data online.	•	•	•	•	•
Regulators should do more to protect my data online.	•	•	•	•	•
I am concerned about my privacy online.	•	•	•	•	•
I would like to know what safeguards are in place in the event of a data breach.	•	•	•	•	•
I would like to know how I may be compensated in the event of a data breach.	•	•	•	•	•
I would like to know what companies are doing to keep my personal data secure.	•	•	•	•	•
I would like to know what the federal government is doing to keep my personal data secure.	•	•	•	•	•

Please indicate how likely you would be to desire the following types of information before clicking through a website's pages

	Very Unlikely	Unlikely	Undecided	Likely	Very Likely
information about the data privacy policies about how your data is used on the site you visited.	•	•	•	•	•
information about how to opt-out of online behavioral tracking used to offer you advertisements based on your browsing history.	•	•	•	•	•
information about what 3rd parties (if any) with which the site shares consumer data.	•	•	•	•	•

Is there any other type of information you would seek out before browsing on a website?

In part 3, we are switching gears to questions about brands.

Please indicate which brand websites you are familiar with.

	Not Familiar At All	Somewhat Unfamiliar	Not Sure	Somewhat Familiar	Very Familiar
BestBuy.com	●	●	●	●	●
Amazon.com	●	●	●	●	●
Walmart.com	●	●	●	●	●
CamerasGalore.com	●	●	●	●	●
Suppliesplus.com	●	●	●	●	●
ComputerMart.com	●	●	●	●	●

Please indicate your level of agreement with the following:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Bestbuy.com meets my expectations.	•	•	•	•	•
I feel confidence in the BestBuy.com brand name.	•	•	•	•	•
BestBuy.com is a brand that never disappoints me.	•	•	•	•	•
BestBuy.com is a brand name that would be honest and sincere in addressing my concerns.	•	•	•	•	•
I could rely on BestBuy.com to solve the problem.	•	•	•	•	•
BestBuy.com would make an effort to satisfy me.	•	•	•	•	•
BestBuy.com would compensate me in some way for the problem with the product I purchased.	•	•	•	•	•

Please indicate your level of agreement with the following:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Amazon.com meets my expectations.	•	•	•	•	•
I feel confidence in the Amazon.com brand name.	•	•	•	•	•
Amazon.com is a brand that never disappoints me.	•	•	•	•	•
Amazon.com is a brand name that would be honest and sincere in addressing my concerns.	•	•	•	•	•
I could rely on Amazon.com to solve the problem.	•	•	•	•	•
Amazon.com would make an effort to satisfy me.	•	•	•	•	•
Amazon.com would compensate me in some way for the problem with the product I purchased.	•	•	•	•	•

Please indicate your level of agreement with the following:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
CamerasGalore.com meets my expectations.	•	•	•	•	•
I feel confidence in the CameraGalor.com brand name.	•	•	•	•	•
CamerasGalore.com is a brand that never disappoints me.	•	•	•	•	•
CamerasGalore.com is a brand name that would be honest and sincere in addressing my concerns.	•	•	•	•	•
I could rely on CamerasGalore.com to solve the problem.	•	•	•	•	•
CamerasGalore.com would make an effort to satisfy me.	•	•	•	•	•
CameraGalore.com would compensate me in some way for the problem with the product I purchased.	•	•	•	•	•

Please indicate your level of agreement with the following:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Walmart.com meets my expectations.	•	•	•	•	•
I feel confidence in the Walmart.com brand name.	•	•	•	•	•
Walmart.com is a brand that never disappoints me.	•	•	•	•	•
Walmart.com is a brand name that would be honest and sincere in addressing my concerns.	•	•	•	•	•
I could rely on Walmart.com to solve the problem.	•	•	•	•	•
Walmart.com would make an effort to satisfy me.	•	•	•	•	•
Walmart.com would compensate me in some way for the problem with the product I purchased.	•	•	•	•	•

Please indicate your level of agreement with the following:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
SuppliesPlus.com meets my expectations.	•	•	•	•	•
I feel confidence in the SuppliesPlus.com brand name.	•	•	•	•	•
SuppliesPlus.com is a brand that never disappoints me.	•	•	•	•	•
SuppliesPlus.com is a brand name that would be honest and sincere in addressing my concerns.	•	•	•	•	•
I could rely on SuppliesPlus.com to solve the problem.	•	•	•	•	•
SuppliesPlus.com would make an effort to satisfy me.	•	•	•	•	•
SuppliesPlus.com would compensate me in some way for the problem with the product I purchased.	•	•	•	•	•

Please indicate your level of agreement with the following:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
ComputerMart.com meets my expectations.	●	●	●	●	●
I feel confidence in the ComputerMart.com brand name.	●	●	●	●	●
ComputerMart.com is a brand that never disappoints me.	●	●	●	●	●
ComputerMart.com is a brand name that would be honest and sincere in addressing my concerns.	●	●	●	●	●
I could rely on ComputerMart.com to solve the problem.	●	●	●	●	●
ComputerMart.com would make an effort to satisfy me.	●	●	●	●	●
ComputerMart.com would compensate me in some way for the problem with the product I purchased.	●	●	●	●	●

Please indicate how much personal risk you felt after being told you have high (low) risk regarding your online data privacy?

	No Risk	.	Some Risk	.	A Lot of Risk
.	●	●	●	●	●

Please indicate how much concern you felt after being told you have high (low) risk regarding your online data privacy?

	No Concern	.	Some Concern	.	A Lot of Concern

Before our calculations, were you previously aware of the high (low) risk your personal data being compromised and used in ways you may find embarrassing or inappropriate?

	Not at all Aware	.	Somewhat Aware	.	Very Aware
.	●	●	●	●	●

Participants were debriefed and given the opportunity to have their data removed from the study.

Appendix B

Main Experiment Questionnaire

For the following questions please indicate how often you are likely to do the following:

	Very Unlikely	Unlikely	Somewhat Unlikely	Undecided	Somewhat Likely	Likely	Very Likely
Have your computer save passwords.	●	●	●	●	●	●	●
Read unsolicited e-mail.	●	●	●	●	●	●	●
Provide a false or fictitious name when registering on a website.	●	●	●	●	●	●	●
Use public wi-fi.	●	●	●	●	●	●	●
Log onto online accounts using public computers.	●	●	●	●	●	●	●
Have a virus checker installed on your computer.	●	●	●	●	●	●	●
Set up your browser to reject unnecessary cookies.	●	●	●	●	●	●	●
Lock your computer when it is not in use.	●	●	●	●	●	●	●
Upgrade your browser to the newest version.	●	●	●	●	●	●	●
Open an email without a subject.	●	●	●	●	●	●	●

Use a password that can be found in the dictionary.	●	●	●	●	●	●	●
Accept unknown "friends" on social networking sites.	●	●	●	●	●	●	●
Make sure online forms are secure before filling them out.	●	●	●	●	●	●	●
Clear computer's cache after browsing	●	●	●	●	●	●	●
Frequently scan your computer for spyware.	●	●	●	●	●	●	●
Use a separate email account that you use solely for the purpose of registering on websites.	●	●	●	●	●	●	●
Save your credit card information in an online store's database.	●	●	●	●	●	●	●

When you get an e-mail from a financial institution asking for information updates, you click the link and fill out their update form.	●	●	●	●	●	●	●
Look for and read privacy statements on the Web.	●	●	●	●	●	●	●
Use anonymizers while browsing the web.	●	●	●	●	●	●	●
Include biographical information about you online (e.g., on Facebook or other site).	●	●	●	●	●	●	●
Use social networking sites.	●	●	●	●	●	●	●
Post on social networking sites.	●	●	●	●	●	●	●

Please indicate your answer to the following questions.

	Never	Rarely	Sometimes	Most of the time	Always
How often do you encounter advertising based on what you have previously searched for?	•	•	•	•	•
How often do you click on advertisements that offer discounts for a product?	•	•	•	•	•

Please indicate approximately how many hours per day you devote to the following activities.

	0 hours	less than an hour	1-2 hours	2-3 hours	3-4 hours	4 or more hours
About how much time do you spend online each day?	•	•	•	•	•	•
About how much time do you spend on social networking sites each day?	•	•	•	•	•	•
About how much time do you spend shopping online each day?	•	•	•	•	•	•

How many purchases would you estimate you have made online in the past month?

- 0
- 1
- 2
- 3
- 4
- 5 or more

What is your gender?

- Male
- Female

What is your age?

Please indicate your highest level of education.

- some high school
- high school/GED
- some college
- college
- some graduate school
- graduate school

Please indicate your yearly household income

- Under 10,001
- 10,001-20,000
- 20,001-40,000
- 40,001-60,000
- 60,001- 80,000
- 80,001 - 100,000
- Over 100,001

Thank you! Please be patient while we calculate your risk quotient.

Participants saw randomly, a high or low risk message.

Please indicate on the scale below your level of awareness of your risk level previous to our short test.

	Not at all Aware	2	3	4	5	6	Very Aware
.	●	●	●	●	●	●	●

Moving on to part 2 of the study.

The second part of the study asks you to tell us a little bit more about your online purchasing habits. Please try to imagine yourself in the following online shopping scenarios.

SCENARIO 1:

Imagine you have decided to add biking to your fitness routine. You have decided to buy a bicycle that costs about $650 and that you believe is a good fit for your biking needs.

You have decided to purchase your new bicycle from (Walmart.com) SuppliesPlus.com.

The following information is available on the SuppliesPlus.com (Walmart.com) website. Please indicate how likely you would be to: seek out and read about the following pieces of information clicking through the website and choosing your new bike.

	Very Unlikely	Unlikely	Somewhat Unlikely	Undecided	Somewhat Likely	Likely	Very Likely
How to place your order.	●	●	●	●	●	●	●
Payment options.	●	●	●	●	●	●	●
How secure the website is.	●	●	●	●	●	●	●
Information the website collects about you.	●	●	●	●	●	●	●
Use of cookies on the website.	●	●	●	●	●	●	●
Rebates.	●	●	●	●	●	●	●
How the site uses pattern recognition to link your purchase history to products you might like.	●	●	●	●	●	●	●
Information the site exchanges with third party advertisers.	●	●	●	●	●	●	●
Defective items.	●	●	●	●	●	●	●
Exchanges.	●	●	●	●	●	●	●
Refunds.	●	●	●	●	●	●	●
Return exceptions.	●	●	●	●	●	●	●
How the site uses your credit card information.	●	●	●	●	●	●	●
Order processing time.	●	●	●	●	●	●	●
How to opt-out of the site's cookie tracking system.	●	●	●	●	●	●	●
How the site ensures consumer data privacy.	●	●	●	●	●	●	●

The website's mobile application privacy options.	•	•	•	•	•	•	•
Contact information in case you have privacy related questions.	•	•	•	•	•	•	•
A pledge of accountability by the company.	•	•	•	•	•	•	•
How your IP address and other information are collected by social media widgets on the site (for example, Facebook or Pinterest icon).	•	•	•	•	•	•	•
Customer reviews about the site.	•	•	•	•	•	•	•
A privacy seal or icon. For example, E-Verify or Better Business Bureau icons.	•	•	•	•	•	•	•

Now, let's move to the second shopping scenario.

SCENARIO 2:

Imagine you are about to go on a once in a lifetime vacation. In preparation for this trip, you plan to buy a new camera to capture all of the important moments. You have decided to buy a camera that costs about $500 and that you believe meets all of your photography needs.

You have decided to purchase your new camera from CamerasGalore.com (BestBuy.com).

The following information is available on the (BestBuy.com) CamerasGalore.com website. Please indicate how likely you would be to seek out and read about the following pieces of information clicking through the website and choosing your new camera.

	Very Unlikely	Unlikely	Somewhat Unlikely	Undecided	Somewhat Likely	Likely	Very Likely
How to place your order.	●	●	●	●	●	●	●
Payment options.	●	●	●	●	●	●	●
How secure the website is.	●	●	●	●	●	●	●
Information the website collects about you.	●	●	●	●	●	●	●
Use of cookies on the website.	●	●	●	●	●	●	●
Rebates.	●	●	●	●	●	●	●
How the site uses pattern recognition to link your purchase history to products you might like.	●	●	●	●	●	●	●
Information the site exchanges with third party advertisers.	●	●	●	●	●	●	●
Defective items.	●	●	●	●	●	●	●
Exchanges.	●	●	●	●	●	●	●
Refunds.	●	●	●	●	●	●	●
Return exceptions.	●	●	●	●	●	●	●
How the site uses your credit card information.	●	●	●	●	●	●	●
Order processing time.	●	●	●	●	●	●	●
How to opt-out of the site's cookie tracking system.	●	●	●	●	●	●	●

How the site ensures consumer data privacy.	•	•	•	•	•	•	•
The website's mobile application privacy options.	•	•	•	•	•	•	•
Contact information in case you have privacy related questions.	•	•	•	•	•	•	•
A pledge of accountability by the company.	•	•	•	•	•	•	•
How your IP address and other information are collected by social media widgets on the site (for example, Facebook or Pinterest icon).	•	•	•	•	•	•	•
Customer reviews about the site.	•	•	•	•	•	•	•
A privacy seal or icon. For example, E-Verify or Better Business Bureau icons.	•	•	•	•	•	•	•

Just a few more questions on this topic

Please indicate how likely you would be to do the following before clicking through a website in the future.

	Very Unlikely	Unlikely	Somewhat Unlikely	Undecided	Somewhat Likely	Likely	Very Likely
Look for an icon that, when clicked, will give you information about how your data is being used.	●	●	●	●	●	●	●
Look for an icon that, when clicked, will give you information about how to opt-out of collection of your online data.	●	●	●	●	●	●	●
Give an email address to a site you do not know.	●	●	●	●	●	●	●
Give an email address to a site that you are familiar with.	●	●	●	●	●	●	●
Give your real name to a familiar site.	●	●	●	●	●	●	●
Give your real name to an unfamiliar site.	●	●	●	●	●	●	●

Use software that hides your computers' identity from websites you visit.	•	•	•	•	•	•	•
Erase some or all of the unwanted cookies on your computer.	•	•	•	•	•	•	•
Check privacy settings on websites on sites you visit in the future.	•	•	•	•	•	•	•
Talk with friends and family about data privacy issues.	•	•	•	•	•	•	•
Check your privacy settings on all of your wireless enabled devices.	•	•	•	•	•	•	•
Ensure sites you visit have privacy safety seals (for example, Better Business Bureau or E-verify icons)	•	•	•	•	•	•	•
Check for customer reviews about the site.	•	•	•	•	•	•	•

Choose not to register on a site because it asks for personal information to get into the site.	•	•	•	•	•	•	•
Search for instructions about how to protect information about yourself on the web.	•	•	•	•	•	•	•

Now, we will switch gears and ask you about online data security.

Please indicate your level of agreement with the following.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
I feel that I have control over my data online.	●	●	●	●	●	●	●
I believe I can opt-out of allowing advertisers and companies to collect my online behavioral data (ie. remembering what sites I visit, remember what I click on in those sites to serve advertising that they believe will be more relevant to me).	●	●	●	●	●	●	●
I can use online privacy tools to remain anonymous online.	●	●	●	●	●	●	●
I understand how my online behavioral data is used online.	●	●	●	●	●	●	●
Data used to serve relevant advertising may be compromised.	●	●	●	●	●	●	●
Data companies collect about me could end up in the hands of criminals.	●	●	●	●	●	●	●

Data companies collect about me might be used in ways that make me feel uncomfortable.	•	•	•	•	•	•	•
Once my data is collected, I have no control over how it is used.	•	•	•	•	•	•	•
I would like to see additional regulation enacted to protect my data privacy online.	•	•	•	•	•	•	•
I would like a new law enacted to protect my data online.	•	•	•	•	•	•	•
Regulators should do more to protect my data online.	•	•	•	•	•	•	•
I am concerned about my privacy online.	•	•	•	•	•	•	•
I would like to know what safeguards are in place in the event of a data breach.	•	•	•	•	•	•	•
I would like to know how I may be compensated in the event of a data breach.	•	•	•	•	•	•	•
I would like to know what companies are doing to keep my personal data secure.	•	•	•	•	•	•	•

I would like to know what the federal government is doing to keep my personal data secure.	•	•	•	•	•	•	•

Please indicate how likely you would be to desire the following types of information before clicking through a website's pages.

	Very Unlikely	Unlikely	Somewhat Unlikely	Undecided	Somewhat Likely	Likely	Very Likely
information about the data privacy policies about how your data is used on the site you visited.	•	•	•	•	•	•	•
information about how to opt-out of online behavioral tracking used to offer you advertisements based on your browsing history.	•	•	•	•	•	•	•
information about what 3rd parties (if any) with which the site shares consumer data.	•	•	•	•	•	•	•

Is there any other type of information you would seek out before browsing on a website?

How much do you trust the following institutions or persons in terms of how well they fulfill their responsibilities in collecting and handling consumer data collected online?

	A Lot	Some	Little	None
The government	•	•	•	•
Individual advertisers	•	•	•	•
The advertising industry	•	•	•	•
Individual brands	•	•	•	•

Please mark your level of agreement or disagreement with the following statements.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
It is safe to believe that in spite of what people say, most people are primarily interested in their own welfare.	•	•	•	•	•	•	•
In dealing with strangers, one is better off being cautious until they have provided evidence that they are trustworthy.	•	•	•	•	•	•	•
Most repairmen will not overcharge even if they think they can get away with it.	•	•	•	•	•	•	•
If you are not careful, others can easily manipulate you.	•	•	•	•	•	•	•
It's important to me to know how a brand website will use my data.	•	•	•	•	•	•	•

In part 3, we are switching gears to questions about brands.

Please indicate which brand websites you are familiar with.

	Not Familiar At All	Somewhat Unfamiliar	Not Sure	Somewhat Familiar	Very Familiar
BestBuy.com	●	●	●	●	●
Amazon.com	●	●	●	●	●
Walmart.com	●	●	●	●	●
CamerasGalore.com	●	●	●	●	●
Suppliesplus.com	●	●	●	●	●
ComputerMart.com	●	●	●	●	●

Please tell us how often you shop at the following:

	Never	Less than Once a Month	Once a Month	2-3 Times a Month	Once a Week	2-3 Times a Week	Daily
SuppliesPlus.com	●	●	●	●	●	●	●
CamerasGalore.com	●	●	●	●	●	●	●

Have you ever read the privacy policy on the following brand websites? (The other condition had the Bestbuy.com/Walmart.com)

	Yes	I don't know	No
CamerasGalore.com	●	●	●
SuppliesPlus.com	●	●	●

Please indicate your level of agreement with the following statements about brand names.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
Brand names inform me about the functional capabilities of a product.	•	•	•	•	•	•	•
Brand names help me decide how well a product will perform.	•	•	•	•	•	•	•
Brand names help me determine the safety of a brand's website.	•	•	•	•	•	•	•

Please indicate your level of agreement with the following:

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
SuppliesPlus.com meets my expectations.	●	●	●	●	●	●	●
I feel confidence in the SuppliesPlus.com brand name.	●	●	●	●	●	●	●
SuppliesPlus.com is a brand that never disappoints me.	●	●	●	●	●	●	●
SuppliesPlus.com is a brand name that would be honest and sincere in addressing my concerns.	●	●	●	●	●	●	●
I could rely on SuppliesPlus.com to solve the problem.	●	●	●	●	●	●	●
SuppliesPlus.com would make an effort to satisfy me.	●	●	●	●	●	●	●
SuppliesPlus.com would compensate me in some way for the problem with the product I purchased.	●	●	●	●	●	●	●

Please indicate your level of agreement with the following.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
CamerasGalore.com meets my expectations.	●	●	●	●	●	●	●
I feel confidence in the CamerasGalore.com brand name.	●	●	●	●	●	●	●
CamerasGalore.com is a brand that never disappoints me.	●	●	●	●	●	●	●
CamerasGalore.com is a brand name that would be honest and sincere in addressing my concerns.	●	●	●	●	●	●	●
I could rely on CamerasGalore.com to solve the problem.	●	●	●	●	●	●	●
CamerasGalore.com would make an effort to satisfy me.	●	●	●	●	●	●	●
CamerasGalore.com would compensate me in some way for the problem with the product I purchased.	●	●	●	●	●	●	●

Please indicate how much personal risk you felt after being told you have high risk regarding your online data privacy?

	No Risk	.	Some Risk	.	A Lot of Risk
.	●	●	●	●	●

Please indicate how much you felt after being told you have high (low) risk regarding your online data privacy?

	No Concern	.	Some Concern	.	A Lot of Concern
.	●	●	●	●	●

What would you say was the primary purpose of this study?

PARTICIPANTS WERE DEBRIEFED

I would like to withdraw all of the answers I provided from this experiment.

- No
- Yes

Appendix 3

High Risk Message

Our calculations show:

Your personal data is at **HIGH RISK** of being stolen or used in a way you may find embarrassing or inappropriate.

Reduce your risk by first understanding how a brand's website uses your data and protects your privacy before clicking through its pages or making a purchase on that site.

Low Risk Message

Our calculations show:

Your personal data is at **LOW RISK** of being stolen or used in a way you may find embarrassing or inappropriate.

Appendix 4

Debriefing Language

Using Heuristic-Systematic Processing Theory To Understand Consumer Shopping Behavior

IRB # 1211667
Study Debriefing

The risk level you were assigned was simulated and NOT based on any real calculation. You were randomly assigned to a risk level that had no connection to the questions you answered at the beginning of the experiment.

Deception was necessary in this study in an effort to create a "real" feeling of risk so that you may (if you were in the high risk group) feel that your data was potentially at risk as a result of the information you provided at the beginning of the study. Theoretically, a feeling of risk is necessary to motivate people to protect their privacy online.

This study is concerned with people paying attention to website privacy policies. Previous studies have found that people do not pay attention to privacy policies and as a result, their consumer data may be used in ways they did not anticipate. One hypothesis this study tests is whether a warning about the risk to a consumer's data will motivate them to desire more information about websites they shop on.

How was this tested?
In this study, you were asked to perform two tasks—filling out demographic information (age, gender, shopping habits), and completing the questions after reading a scenario about shopping online. One group saw a warning page after the completion of the demographic questions that said their data was at high risk, while the other group saw a page that indicated that their data was low risk.

Hypotheses and main questions:
I expect to find that those who received the warning about their data being at risk are going to be more likely to ask for additional information about the sites they are asked to assume they are making a purchase from in the scenarios than those who did not get a warning.

I am also interested in the influence of brand familiarity on the effects of the warning. Some participants received familiar brands in their scenarios while others did not. I suspect that when people are shopping on a familiar brand's website, they will be less likely to be concerned about data privacy.

Why is this important to study?
There are many times when consumers do not know how their data is being used online. This study may help to advance policy initiatives in an effort to make sure that consumers are clearly informed and/or notice the policies on websites that will offer them information about potential risks.

Want to remove your data from the study?
If you would like to remove your data from the study, there will be a place to click following this debrief. Please click that box if you would like your data to be removed from the study.

What if you want to know more?

If you would like to receive a report of this research when it is completed (or a summary of the findings), please contact Heather Shoenberger at hrskv9@mail.missouri.edu or Dr. Esther Thorson at thorsone@mail.missouri.edu

If you have concerns about your rights as a participant in this experiment, please contact the Campus IRB at 573-882-9585.

Thank you again for your participation.

REFERENCES

Aaker, David A., and Erich Joachimsthaler. "The brand relationship spectrum."*California Management Review* 42, no. 4 (2000): 8-23.

Averbeck, Joshua M., Allison Jones, and Kylie Robertson. "Prior knowledge and health messages: An examination of affect as heuristics and information as systematic processing for fear appeals." *Southern Communication Journal* 76, no. 1 (2011): 35-54.

Bachman, Katy. (2013) "Users More Likely to Click On Ads With AdChoices Icon: DAA poll says it's good for brands." *AdWeek.* Retrieved from: http://www.adweek.com/news/technology/users-more-likely-click-ads-adchoices-icon-153617.

Bauer, Raymond A. "Consumer behavior as risk taking." *Dynamic marketing for a changing world* 398 (1960).

Biek, Michael, Wendy Wood, and Shelly Chaiken. "Working knowledge, cognitive processing, and attitudes: On the determinants of bias." *Personality and Social Psychology Bulletin* 22, no. 6 (1996): 547-556.

Brossard, Dominque, Dietram Scheufele, Eunkyung Kim and Bruce Lewenstein (2009). "Religiosity as a perceptual filter: examining processes of opinion formation about nanotechnology," *Public Understanding of Science, 18*(5), 546-558. doi. 10.1177/0963662507087304.

Buhrmester, Micheal, Tracy Kwang, and Samuel D. Gosling. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? Perspectives on Psychological Science, 6(1):3–5, January 2011.

Campbell, Damon E., and Ryan T. Wright. "Shut-up I don't care: Understanding the role of relevance and interactivity on customer attitudes toward repetitive online advertising." *Journal of Electronic Commerce Research* 9, no. 1 (2008).

Campbell, Margaret C., and Kevin Lane Keller. "Brand familiarity and advertising repetition effects." *journal of Consumer Research* 30, no. 2 (2003): 292-304.

Chaiken, Shelly. "Heuristic versus systematic information processing and the use of source versus message cues in persuasion." *Journal of personality and social psychology* 39, no. 5 (1980): 752.

_____. "Physical appearance and social influence." In *Physical appearance, stigma, and social behavior: The Ontario Symposium*, vol. 3, pp. 143-177. 1986.

_____, Akiva Liberman and Alice H. Eagly. "Heuristic and systematic information processing within and beyond the persuasion context." *Unintended thought* 212 (1989).

_____, and Durairaj Maheswaran. "Heuristic processing can bias systematic processing: effects of source credibility, argument ambiguity, and task importance on attitude judgment." *Journal of personality and social psychology* 66, no. 3 (1994): 460.

_____,and Charles Stangor. "Attitudes and attitude change." *Annual review of psychology* 38, no. 1 (1987): 575-630.

Claypool, Heather M., Diane M. Mackie, Teresa Garcia-Marques, Ashley Mcintosh, and Ashton Udall. "The effects of personal relevance and repetition on persuasive processing." *Social Cognition* 22, no. 3 (2004): 310-335.

Consumer Data Privacy In a Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Digital Global Economy. 2012. Available from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Delgado-Ballester, Elena, Jose Luis Munuera-Aleman, and Maria Jesus Yague-Guillen. "Development and validation of a brand trust scale." *International Journal of Market Research* 45, no. 1 (2003): 35-54.

DelVecchio, Devon. "Consumer perceptions of private label quality: the role of product category characteristics and consumer use of heuristics." *Journal of Retailing and Consumer Services* 8, no. 5 (2001): 239-249.

Dholakia, Utpal M. "A motivational process model of product involvement and consumer risk perception." *European Journal of marketing* 35, no. 11/12 (2001): 1340-1362.

Eagly, Alice H., and Shelly Chaiken. *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers, 1993.

E-marketer (2013). "Retail Ecommerce Set to Keep a Strong Pace Through 2017." Retrieved from: http://www.emarketer.com/Article/Retail-Ecommerce-Set-Keep-Strong-Pace-Through-2017/1009836.

_____ (2014). "Digital Ad Spending Worldwide To Hit $137.53 Billion in 2014." Retrieved from: http://www.emarketer.com/Article/Digital-Ad-Spending-Worldwide-Hit-3613753-Billion-2014/1010736.

Faul, Franz, Edgar Erdfelder, Albert-Georg Lang, and Axel Buchner. "G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences." *Behavior research methods* 39, no. 2 (2007): 175-191.

Freitag, Markus, and Marc Bühlmann. "Crafting Trust The Role of Political Institutions in a Comparative Perspective." *Comparative Political Studies* 42, no. 12 (2009): 1537-1566.

Fuchs, Erin. (2012) The Most High Profile Executive Suicides of the Recent Years. Business Insider. Retrieved from: http://www.businessinsider.com/the-most-high-profile-business-people-who-turned-to-suicide-during-scandals-2012-8?op=1.

Galli, Maria, and Gerald Gorn. "Unconscious transfer of meaning to brands."*Journal of Consumer Psychology* 21, no. 3 (2011): 215-225.

Gigerenzer, Gerd. "Why heuristics work." *Perspectives on psychological science* 3, no. 1 (2008): 20-29.

____ and Wolfgang Gaissmaier. "Heuristic decision making." *Annual review of psychology* 62 (2011): 451-482.

Goel, Vindu (2014) "Facebook To Let Users Alter Their Ad Profiles." *The New York Times*. Retrieved from: http://www.nytimes.com/2014/06/13/technology/facebook-to-let-users-alter-their-ad-profiles.html?_r=0.

Goodman, Joseph K., Cynthia E. Cryder, and Amar Cheema. "Data collection in a flat world: The strengths and weaknesses of Mechanical Turk samples."*Journal of Behavioral Decision Making* 26, no. 3 (2013): 213-224.

Griffin, Robert J., Sharon Dunwoody, and Kurt Neuwirth. "Proposed model of the

relationship of risk information seeking and processing to the development of preventive behaviors." *Environmental research* 80, no. 2 (1999): S230-S245.

Haidt, Jonathan. *The righteous mind: Why good people are divided by politics and religion*. Random House LLC, 2013.

Han, Peter, and Angus Maclaurin. "Do consumers really care about online privacy?." *Marketing Management* 11, no. 1 (2002): 35-38.

Hoyer, Wayne D., and Steven P. Brown. "Effects of brand awareness on choice for a common, repeat-purchase product." *Journal of Consumer Research* (1990): 141-148.

Joinson, Adam N., Ulf- Dietrich Reips, Thomas Buchanan and Carina Schofield (2010). "Privacy, Trust, and Self-Disclosure Online," *Human-Computer Interaction, 25*(1), 1-24. doi: 10.1080/07370020903586662.

Kahlor, LeeAnn, Sharon Dunwoody, Robert J. Griffin, Kurt Neuwirth, and James Giese. "Studying Heuristic-Systematic Processing of Risk Communication."*Risk Analysis* 23, no. 2 (2003): 355-368.

Kapferer, Jean-Noël. "The post-global brand." *The Journal of Brand Management* 12, no. 5 (2005): 319-324.

Langenderfer, Jeff, and Anthony D. Miyazaki. "Privacy in the information economy." *Journal of Consumer Affairs* 43, no. 3 (2009): 380-388.

Langer, Ellen J., and Robert P. Abelson. "The semantics of asking a favor: How to succeed in getting help without really dying." *Journal of Personality and Social Psychology* 24, no. 1 (1972): 26.

Leon, Pedro, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. "Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 589-598. ACM, 2012.

Luhmann, Niklas. *Trust; and, Power: two works by Niklas Luhmann*. Chichester: Wiley, 1979.

Maheswaran, Durairaj, Diane M. Mackie, and Shelly Chaiken. "Brand name as a

heuristic cue: The effects of task importance and expectancy confirmation on consumer judgments." *Journal of Consumer Psychology* 1, no. 4 (1992): 317-336.

Marcoux, Alexei M. "Much ado about price discrimination." *Journal of Markets & Morality* 9, no. 1 (2012).

Maris, David (2012) A Drug Recall That Should Frighten Us All About the FDA. *Forbes.com*. Retrieved from: http://www.forbes.com/sites/davidmaris/2012/10/10/fda-recall-points-to-serious-problems-at-the-fda/

McDonald, Aleecia M., and Lorrie Faith Cranor. "Americans' attitudes about internet behavioral advertising practices." In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, pp. 63-72. ACM, 2010.

McRoberts, Flynn and Cam, Simpson. (2002). "Ex-Enron's excec's suicide note released."*Chicago Tribube.* Retrieved from: http://articles.chicagotribune.com/2002-04-12/business/0204120223_1_suicide-note-ex-enron-baxter.

Metzger, Miriam J. (2007). "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication, 12*(2), 335-361. doi: 10.1111/j.1083-6101.2007.00328.x.

Milne, George R. (1997), "Consumer Participation in Mailing Lists: A Field Experiment," Journal of Public Policy &Marketing, 16 (Fall), 298-309.

_____, Lauren I. Labrecque, and Cory Cromer. "Toward an understanding of the online consumer's risky behavior and protection practices." *Journal of Consumer Affairs* 43, no. 3 (2009): 449-473.

_____., Jason A. Gabisch, Ereni Markos, and Joseph E. Phelps. "Changes in Consumer Willingness to Provide Information over the Last Decade: A Cohort Analysis." *International Journal of Integrated Marketing Communications* 4, no. 2 (2012).

Miyazaki, Anthony D., and Ana Fernandez. "Consumer perceptions of privacy and security risks for online shopping." *Journal of Consumer Affairs* 35, no. 1 (2001): 27-44.

___ and Sandeep Krishnamurthy. "Internet seals of approval: Effects on online privacy policies and consumer perceptions." *Journal of Consumer Affairs* 36, no. 1 (2002): 28-49.

Nelson, Douglas A., and Lisa J. Croner. "Song categories and their functions in the field sparrow (Spizella pusilla)." *The Auk* (1991): 42-52.

Neuwirth, Kurt, Sharon Dunwoody, and Robert J. Griffin. "Protection motivation and risk communication." *Risk Analysis* 20, no. 5 (2000): 721-734.

Nooteboom, Bart. "Forms, sources and processes of trust." *Handbook of trust research* (2006): 247.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne. "The privacy paradox: Personal information disclosure intentions versus behaviors." *Journal of Consumer Affairs* 41, no. 1 (2007): 100-126.

Nowak, Glen J., and Joseph Phelps. "Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs." *Journal of Direct Marketing* 6, no. 4 (1992): 28-39.

Okazaki, Shintaro, Hairong Li, and Morikazu Hirose. "Consumer privacy concerns and preference for degree of regulatory control." *Journal of Advertising* 38, no. 4 (2009): 63-77.

"Online Tracking and Behavioral Profiling." (2014) *Electronic Privacy Information Center*. Retrieved from: http://epic.org/privacy/consumer/online_tracking_and_behavioral.html.

Paolacci, Gabriele, Jesse Chandler, and Panagiotis G. Ipeirotis. "Running experiments on amazon mechanical turk." *Judgment and Decision making* 5, no. 5 (2010): 411-419.

Park, C. Whan, and V. Parker Lessig. "Familiarity and its impact on consumer decision biases and heuristics." *Journal of consumer research* (1981): 223-231.

Petty, Richard E., and John T. Cacioppo. "The elaboration likelihood model of persuasion." *Advances in experimental social psychology* 19 (1986): 123-205.

Poddar, Amit, Jill Mosteller, and Pam Scholder Ellen. "Consumers' rules of engagement in online information exchanges." *Journal of Consumer Affairs* 43, no. 3 (2009): 419-448.

Podesta, John, Penny, Pritzker, Ernest Moniz, John Holdren, Zients, Jeffrey (2014). "Big Data Seizing Opportunities, Preserving Values." *Executive Office of the President.* Retrieved:from:http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

Putnam, Robert. "The prosperous community: social capital and public life." *The american prospect* 13, no. Spring), Vol. 4. Available online: http://www. prospect. org/print/vol/13 (accessed 7 April 2003 (1993).

Reeves, Byron, and Seth Geiger. "Designing experiments that assess psychological responses to media messages." *Measuring psychological responses to media messages* (1994): 165-180.

Richins, Marsha, and Teri Root-Schaffer. "The Role of Involvement and Opinion Leadership in Consumer Word-of-Mouth: An Implicit Model Made Explicit." *Advances in Consumer Research* 25 (1998): 32-36.

Rifon, Nora J., Robert LaRose, and SEJUNG CHOI. "Your privacy is sealed: effects of web privacy seals on trust and personal disclosures." *Journal of Consumer Affairs* 39, no. 2 (2005): 339-362.

Rohm, Andrew J., and George R. Milne. "Emerging marketing and policy issues in electronic commerce: attitudes and beliefs of Internet users." In *Marketing and public policy proceedings*, vol. 8, pp. 73-9. HarperBusiness, 1998.

Rotfeld, Herbert Jack. "Privacy Crimes, Annoyances and Self-Defeating Business Practices." *Journal of Consumer Affairs* 43, no. 3 (2009): 538-542.

Rotter, Julian B. (1967), "A New Scale for the Measurement of Interpersonal Trust," Journal of Personality, 35 (4), 651-65.

Sableman, M., Shoenberger, H., Thorson, E. (August 2013). Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates. *Media Law Resource Center Bulletin.*

Sanger, David and Steve, Lohr (2014) "Call for limits of web data on consumers." *The New York Times*. Retrieved from: http://www.nytimes.com/2014/05/02/us/white-house-report-calls-for-transparency-in-online-data-collection.html.

Sheehan, Kim Bartel, and Mariea Grubbs Hoy. "Dimensions of privacy concern among online consumers." *Journal of Public Policy & Marketing* 19, no. 1 (2000): 62-73.

_____, and Mariea Grubbs Hoy. "E-mail surveys: response patterns, process and potential." In Proceedings of the conference-American Academy of Advertising, pp. 231-231. American Academy of Advertising, 1997.

_____, and Mariea Grubbs Hoy. "Flaming, complaining, abstaining: How online users respond to privacy concerns." *Journal of advertising* 28, no. 3 (1999): 37-51.

Sheth, Jagdish N., and M. Venkatesan. "Risk-reduction processes in repetitive consumer behavior." *Journal of Marketing Research* (1968): 307-310.

Shoenberger, Heather and Esther Thorson. "Prediction of Perceived Online Shopping Benefits and Risks from Trust and Knowledge of Targeting." To be presented at The American Academy of Advertising conference. Atlanta, GA, 2014.

Siegrist, Michael. "The influence of trust and perceptions of risks and benefits on the acceptance of gene technology." *Risk analysis* 20, no. 2 (2000): 195-204.

Simmel, Georg. "The philosophy of money, trans. Tom Bottomore and David Frisby." *London: Routledge & Kegan Paul* 236 (1978): 232.

Smit, Edith G., Guda Van Noort, and Hilde AM Voorveld. "Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe." *Computers in Human Behavior* 32 (2014): 15-22.

Ter Huurne, Ellen, and Jan Gutteling. "Information needs and risk perception as predictors of risk information seeking." *Journal of Risk Research* 11, no. 7 (2008): 847-862.

Tracking Cookie (2014) PCMag.com. Retrieved from: http://www.pcmag.com/encyclopedia/term/56150/tracking-cookie

Trumbo, Craig W. "Heuristic-Systematic Information Processing and Risk

Judgment." *Risk Analysis* 19, no. 3 (1999): 391-400.

Turner, Monique Mitchell, Rajiv N. Rimal, Daniel Morrison, and Hyojin Kim. "The role of anxiety in seeking and retaining risk information: Testing the risk perception attitude framework in two studies." *Human Communication Research*32, no. 2 (2006): 130-156.

Turow, Joseph, and Michael Hennessy. "Internet privacy and institutional trust insights from a national survey." *New media & society* 9, no. 2 (2007): 300-318.

_____, Joseph, King, Jennifer, Hoofnagle, Chris Jay, Bleakley, Amy, and Hennessy, Michael. (2009).“Americans Reject Tailored Advertising and the Three Activities that Enable It.” Availab;e at SSRN: http://ssm.com/abstract=1478214.

Uleman, James S., and John A. Bargh, eds. *Unintended thought*. Guilford Press, 1989.

Wang, Paul, and Lisa A. Petrison. "Direct marketing activities and personal privacy. A consumer survey." *Journal of Direct Marketing* 7, no. 1 (1993): 7-19.

What They Know. (2010-2012). Retrieved from http://online.wsj.com/public/page/what-they-know-digital-privacy.html.

Yang, Z. J., Aloe, A. M. & Feeley, T. H. (2014). Risk information seeking and processing model: A meta-analysis. *Journal of Communication.*

Yap, Jo En, Michael Beverland, and Liliana Bove. "A conceptual framework of the causes and consequences of the privacy paradox." In *The Australian and New Zealand Marketing Academy (ANZMAC) Conference 2009 Proceedings*, pp. 1-9. Melbourne, VIC: Monash University, 2009.

Zajonc, Robert B. "Attitudinal effects of mere exposure." *Journal of personality and social psychology* 9, no. 2p2 (1968): 1.

Zhang, Lixuan, Robert Pavur, Paul York, and Clinton Amos. "Testing a Model of Users' Web Risk Information Seeking Intention." *Informing Science* 16 (2013).

VITA

Heather Shoenberger received her M.A. in Journalism and J.D. from the University of Missouri in 2006. She received her B.A in Psychology and Creative Writing from Drury University in 2002 where she was an All-American swimmer. She has worked as an editor at Bulletin News Network, which publishes the White House News Summary and daily news briefings for various agencies and corporate clients. Shoenberger's research focuses on strategic communication, specifically issues surrounding online interest-based advertising. Other areas of interest include media psychology, privacy, and legal policy issues as they pertain to advertising. She will begin as an assistant professor of advertising at the University of Oregon in the fall of 2014.