ANTECEDENTS AND OUTCOMES OF PERCEIVED CREEPINESS IN ONLINE PERSONALIZED COMMUNICATIONS

by

ARLONDA M. STEVENS

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Weatherhead School of Management

Designing Sustainable Systems

CASE WESTERN RESERVE UNIVERSITY

May, 2016

CASE WESTERN RESERVE UNIVERSITY

SCHOOL OF GRADUATE STUDIES

We hereby approve the thesis/dissertation of

Arlonda M. Stevens

candidate for the degree of Doctor of Philosophy.*

Committee Chair

Richard J. Boland, Jr., Ph.D., Case Western Reserve University

Committee Member

Mary Culnan, Ph.D., Professor Emeritus, Bentley University

Committee Member

Kalle Lyytinen, Ph.D., Case Western Reserve University

Committee Member

Casey Newmeyer, Ph.D., Case Western Reserve University

Date of Defense

March 2, 2016

*We also certify that written approval has been obtained

for any proprietary material contained therein.

Dedication

I dedicate this study of perceived creepiness to all who have received that unanticipated personal communication or had that interaction or encounter with technology that led them to say, “Now that was *creepy*!”

Everything that we see is a shadow cast by that which we do not see.
(Dr. Martin Luther King, Jr.)

Table of Contents

List of Tables

List of Figures

Acknowledgements

It is hard to believe that I have completed my four-year journey in the DM/Ph.D. Program at Case Western Reserve University. What a transformational journey it has been. I now think differently, lead differently and manage differently. It has been an honor and a privilege to be a part of what has to be one of the best programs of this type in the country. I am truly grateful to Dr. Lyytinen, the faculty and staff, along with Marilyn Chorman and Sue Nartker that make this program what it is today—EXCELLENT!

It is difficult to put into words how profoundly grateful I am for all of those who have supported and encouraged me along the way. While all of the faculty have contributed to my growth and provided feedback on my research on perceived creepiness, I owe special gratitude to my Committee members, Dr. Mary Culnan, Dr. Kalle Lyytinen, Dr. Casey Newmeyer, and my Committee chair, Dr. Richard Boland. Thanks also to Dr. James Gaskin, who provided assistance with my first quantitative study. Without the help of Dr. Culnan providing her subject area expertise in the field of Privacy, my research would not have progressed as it has over the past four years. She has been with me since the beginning when I initially mentioned that I wanted to study "creepiness". She has been a big support and has pushed me to think in a scholarly manner.

What can I say about Dr. Boland? He has been A-1 since day 1. I appreciate him believing in me and encouraging me to develop my research into what it is today. Thanks, Dick!

I also owe a ton of thanks to my classmates, all of whom embraced my topic and provided feedback along with their own "creepy" encounters. All of my classmates are dedicated practitioners and amazing scholars. I have learned so much from all of you. Iron sharpens iron! Thanks for the memories. Much love to you all.

Special thanks to Alexis Antes and Casey Mathews for their editing skills and ensuring that my writing is presented with the utmost quality.

I also want to thank my distinguished colleagues at PNC who have also been supportive and frequently checked in with me to see how things were going: Jennifer Davis, Stephanie Psenicka, Toni Baker, Christine Riggenbach, Brad Chocola, and my Privacy mentors—Alice Duke and Sok Woo Yoon.

Where would I be without my "front row"? These people have encouraged me, have been empathetic, endured me not always being available to go out and have fun, endured me saying, "I have to work on my paper", yet have been there every step of the way, each in their own special way. Acknowledging my "front row"—Collette Laisure, Robbin Taylor, Traci Mitchell, Alaina Carpenter, Sheila Webb, Reecella Diggs, Joi Wilson, and my Fisk University compadres.

Next, I thank my family: my mother, Mildred Martin, who would check on me every day to make sure that everything was ok, my sisters Angela and Valerie, my aunt and cousins, particularly Dr. Melodie Mayberry-Stewart and Jay Mayberry, who were able to attend my dissertation proposal defense.

Last but certainly not least, special thanks to my husband, Julio, and especially my children, Jasmine, Julio II, and Jada, who have been my inspiration. They have been very patient, supportive and understanding. I hope that I have set an example for them to be lifelong learners and to know that it is never too late to pursue your dreams. Love you all to pieces!

ALL TO HIM!

Antecedents and Outcomes of Perceived Creepiness in Online Personalized Communications

Abstract

By

ARLONDA M. STEVENS

In an effort to deepen customer relationships (Relationship Marketing), marketers and online firms deliver personalized communications based on a consumers' digital footprint and other Big Data that they think will improve its effect; but the personalized messages are sometimes perceived to be "creepy" by the recipient. Marketers are admonished to not be creepy, but, there is not a unified definition of what creepy is or isn't, nor have the factors leading to perceived creepiness been clearly identified—there is a common feeling of discomfort, but no unified definition. The goal of this study is to address three research questions. First, what is creepy? Second, what factors lead to perceived creepiness? And third, can a scale to measure perceived creepiness be operationalized and used to validate those factors?

I conducted a three-part; sequential, mixed methods study to define perceived creepiness and to identify the antecedents and consequences of perceived creepiness in personalized online messages. The study confirmed that transparency by the firm about their data collection, use and sharing practices and that enabling the consumer to exercise control over the collection, use and sharing of their personal information (including the ability to opt–out of personalized messages) are antecedents of perceived creepiness. Also, whether the message was “in context” or “out of context” had an effect on if the message was perceived to be creepy. It also suggests that trust in the sender has a direct effect on perceived creepiness; and perceived creepiness has a negative effect on customer satisfaction, which can harm brand reputation, sales, and revenue.

This research makes a scholarly contribution by providing a theoretical framework for a Theory of Perceived Creepiness. It also makes a contribution to practice by providing marketers with an understanding of what leads to perceived creepiness, so that they can take action to avoid negative effects of personalized communication on customer satisfaction.

Keywords: creepy; creepy marketing; personalized communication; transparency; control; Creepy Quadrant; online information privacy concerns; online behavioral advertising; data privacy; trust.

CHAPTER 1: INTRODUCTION

Data. Data. Data. In the not too distant past, location was all that mattered; however, in today's information-based society, data is increasingly all that really matters. It's all about the data. And not just any data, its consumers' personal data that has the most value to those firms that seek to increase profits through personalized[1] messages, which are communications tailored to a current or potential consumer based on knowledge about them (Adomavicius & Tuzhilin, 2005). Relationship marketing, which is based on establishing a relationship with the consumer or customer to increase retention and customer satisfaction, has overtaken product and transaction-based marketing, such that, marketers are keenly interested to learn more about the consumer: their likes, dislikes, interests, demographic information and their online and offline behaviors. Every day, consumers provide marketers and other interested parties with the data to learn about them by engaging in transactions that leave behind tremendous amounts of personal information and create a large and growing digital footprint. From the moment a person wakes up in the morning until they go to sleep at night, almost every detail of life is being captured through their phone activity, text messages, Internet searches, purchases, postings on social media and location at any moment in time. The ability to mine and perform data analytics on this information presents companies with

[1] For our research purposes, personalization and personalized messages are used interchangeably. Messages refer to advertisements, tailored customer experiences and interactions as well as other customer communication where personal information is used to determine the recipient of the message or the content of the message. Personalization "refers to the customization of some or all the elements of the marketing mix to an individual level" (Montgomery & Smith, 2008: 4). Further, "personalization is the use of technology and customer information to tailor electronic commerce interactions between a business and each individual customer. Using information either previously obtained or provided in real time about the customer, the exchange between the parties is altered to fit that customer's stated needs, as well as needs perceived by the business based on the available customer information" (Adomavicius & Tuzhilin, 2005).

opportunities to learn, infer and create knowledge about consumers that could not have been done otherwise. Firms are capitalizing on data that was provided to them for one purpose, yet using it for something else (Culnan, 1993). Marketers are now able to combine this data with insights gained from consumers' digital footprints of online and offline behaviors to create personalized messages such as direct communications, online advertisements, and tailored customer experiences.

Companies believe that personalized messages help to deliver the right message to the right person at the right time in the right way, all the while being relevant to the individual consumer (Double Click Website, 2011). Further, companies hope that personalized messages will enable them to build relationships with customers who will then become loyal and satisfied with their product or service (Chellappa & Sin, 2005; Gwinner, 1997). The data equation looks like this:

(Big Data + Knowledge of Online Behaviors) x Data Analytics =Personalized Communications

Statement of the Problem

"Now that's creepy!" This phrase has become common among consumers in response to personalized communications that used their personal data, along with knowledge of their offline and online behaviors, in an unexpected way to deliver a personalized message. Zappos shoe ads "follow" you on the Internet (Helft & Vega, 2010); Amazon provides you with items that you may be interested in buying or recommends music and books based on your current library; Facebook shows you people that you may know, and you know all of them; Facebook also sends you ads based on your "likes" and knows what you are watching on television. These are all examples of personalized messages or online behavioral advertising perceived to be creepy by some consumers. One of the more dramatic examples, which many agreed was creepy, was the infamous Target incident. Through the data collection efforts of Target, they were able to mine data and glean the unique consumer buying habits of women who had signed up for Target's baby registries. From this analysis, they were able to predict that a teenage girl was pregnant. In this case, Target sent the young girl coupons for baby-related items. Her father questioned the store manager as to why his daughter was receiving these coupons only to find out later that his daughter was indeed pregnant. Target discovered that the teen was pregnant before her father did (Hill, 2012)! The fact that Target knew so much about their customers' buying habits and about their unannounced pregnancies, "*creeped*" people out (Hill, 2012).

Recognizing the benefits of personalized communications such as relevant messages, coupons as in the case of Target, loyalty rewards and other perks (Gwinner, 1997) consumers' perception of online behavioral advertising (OBA) has been described as smart and useful. But at the same time, it has been described as scary or creepy (Ur, Leon, Cranor, Shay, & Wang, 2012). What is it about these incidents that people describe as creepy? What happened or didn't happen that led a personalized communication to be perceived as creepy? Which behavioral advertising and personalized messages are clever and which are creepy? The question has even been posed: "Is Personalization Creepy"?[2] To adequately address these questions, one must first understand what creepy means and ask, "What is creepy?" Then one can ask, "What makes a personalized message to be perceived as creepy?" What is *really* behind perceived creepiness? And what are the impacts on marketers or the firm when they deliver what they think is a relevant ad, but it

[2] http://blog.hubspot.com/marketing/marketing-personalization-creepy

is perceived to be creepy by the consumer? These questions provide the basis for my research.

Marketers are admonished to not be creepy, as evidenced by a search on Google showing several practitioner-oriented articles discussing marketing, personalization and creepy: “Is Marketing Getting Too Creepy?”[3], “Be relevant, Not creepy.”[4], “Targeted Marketing: Helpful or Creepy?”[5], “The Line Between Creepy and Effective Marketing.”[6], and “Personalization: Creepy vs. Brilliant.”[7], just to name a few. The problem of practice is that Marketers cannot avoid “creepy” if they do not know what it means, or if the factors that constitute perceived creepiness have not been clearly identified. Furthermore, they cannot avoid the downstream impacts or unintended consequences of delivering personalized communications if they don’t know what creepy is and measures that can be taken to avoid it.

Despite all of the rhetoric around “creepiness”, the creepy phenomena has not been extensively explored in extant academic literature within the context of personalized messages. Barnard (2014) explores creepiness within the context of purchase intentions, and Moore et al. (2015) researches creepy marketing and defines it based on three dimensions: invasion of privacy, stalking behavior and violation of social norms. Tene and Polonetsky (2013) put forth a theory of creepy that centers primarily on the technology that invokes a creep factor; (Keenan, 2014)speaks of creepy from a

[3] http://blog.hubspot.com/blog/tabid/6307/bid/33332/Is-Marketing-Getting-Too-Creepy.aspx
[4] http://www.dmnews.com/digital-marketing/be-relevant-not-creepy/article/256050/
[5] http://www.enterrasolutions.com/2015/04/targeted-marketing-helpful-creepy.html
[6] http://www.cmswire.com/cms/digital-marketing/the-line-between-creepy-and-effective-marketing-026693.php
[7] http://www.socialmediatoday.com/marketing/2015-03-10/personalization-creepy-vs-brilliant

technological perspective in his book, *Technocreep*, and creepiness is also researched in terms of whether it should be used as the standard of privacy harm (Thierer, 2013). In addition to these studies, other research on creepiness focuses on creepy people (Kotsko, 2015; McAndrew & Koehnke, 2013) Zombies (Kuhlman, 2011), and the Uncanny Valley (Chaminade, 2007; Watson, 2014). The "uncanny valley" was first identified by Mori (Mori, MacDorman, & Kageki, 2012; Mori, 1970) as an eerie or discomforting feeling about robots that look and take on features of humans making them look too realistic. The "uncanny valley" has become a term used my many theorists to describe that unsettling feeling that some technology seems to know us better than we know ourselves (Watson, 2014). Some have even suggested that we are living in the "uncanny valley of Internet advertising" (Manjoo, 2012).

Creepy is hard to describe and often falls under the guise of "I know it when I see it" (Stewart, 1964: 184). To that end, scholars have not developed a universal definition or theory of creepy, nor have they identified and explained the factors that lead to perceptions of creepiness.

Based on the increase in the number of articles and discussions of the "creep factor", it seems as if concerns are beginning to emerge about the "creepiness", privacy invasiveness, lack of transparency and opaque data practices (Camarinha-Matos & Goes, 2013) and lack of consumer control over their data. In a recent study, 91% of adults in the United States say consumers have lost control over how their personal information is collected and used by companies (Madden, 2014a). A more recent report by TRUSTe/National Cyber Security Alliance (TRUSTe/National Cyber Security Alliance, 2016) asserts that 68% of people are more concerned about not knowing how their personal information is collected online than losing their principle income (57%). Companies are able to collect, track, use and share information regarding consumers, oftentimes without their knowledge, for purposes or in ways that they did not originally intend, which Culnan (1993) refers to as secondary use of information, often resulting personalized messages that are sometimes perceived to be creepy. Finally, elements of a message that are perceived as being "out of context" and not "in context" with the communication setting or the norms associated with information flow can result in perceived creepiness. Most often, we are socialized as to how we should view and respond to certain types of data from various sources. Consumers usually have expectations of what is normal and acceptable uses of data and would probably be categorized as "within context"; however, anything outside of the norm of what we as consumers would expect would shift our perspective to which these messages would then be categorized as "out of context." According to Nissenbaum (2009), context or contextual integrity refers to "structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends purposes)" (p. 132).

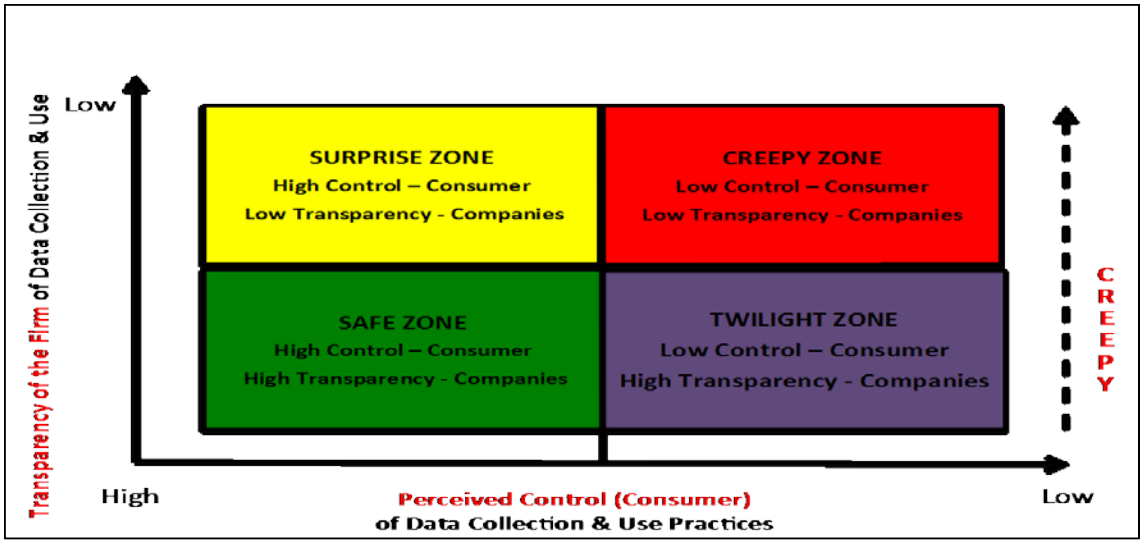
In order to better understand perceived creepiness and its antecedents and consequences or impacts, the problems described above must be addressed and my research attempts to address these issues.

Purpose and Objective of the Research

The overall objective of this research is to identify the antecedents and consequences of perceived creepiness as experienced with online personalized communications. However, in order to address the issue of personalization being perceived as creepy, we must first understand “creepy” what it is, its antecedents and what does it *really* mean when we describe a personalized communication, advertisement or tailored customer experience as “creepy”? Could it be that the term creepy is a façade or crutch (Selinger, 2012) for lack of transparency or something deeper like fear of the unknown, betrayal by a trusted company, a violation of privacy, a lack of control by the consumer over how their personal data is being collected, used and shared, or a breach of the social contract between the firm and the consumer? Or could it be that the message was out of context given the consumers’ expectations regarding norms about information flow (Nissenbaum, 2009)? Given this backdrop of inconsistencies and gaps in our understanding of perceived creepiness, there was an opportunity to develop a foundational, integrated framework to form the basis for a Theory of Perceived Creepiness (TPC).

My sequential mixed methods (Creswell & Plano Clark, 2011) research study is comprised of three distinct studies following a qualitative, quantitative, quantitative sequence. Through the three studies, I sought to further understand perceived creepiness and address various dimensions of the overarching question “What Is Creepy?” Aside from the first study, the findings from one study informed the research questions and inquiry for the next study. My first study was an exploratory study, where I was able to develop a definition of creepy (an emotional reaction to an experience, interaction, technology or unsolicited communication where personal information has been collected with your knowledge or unknowingly and used in an unexpected or surprising manner invoking negative feelings) and identify factors (online information privacy concerns, perceived anonymity, perceived surveillance, transparency and control) that may lead to perceived creepiness based on the collective responses gathered from conducting semi-structured interviews. I also developed the Creepy Quadrant, which is a visual depiction of the inter-relationship between two of the most dominant themes identified in study one: transparency and control (Figure 1).

Figure 1. The Creepy Quadrant


Transparency of the Firm of Data Collection & Use
Low
High
SURPRISE ZONE
High Control – Consumer
Low Transparency - Companies
CREEPY ZONE
Low Control – Consumer
Low Transparency - Companies
SAFE ZONE
High Control – Consumer
High Transparency - Companies
TWILIGHT ZONE
Low Control – Consumer
High Transparency - Companies
CREEPY
Perceived Control (Consumer)
of Data Collection & Use Practices
Low

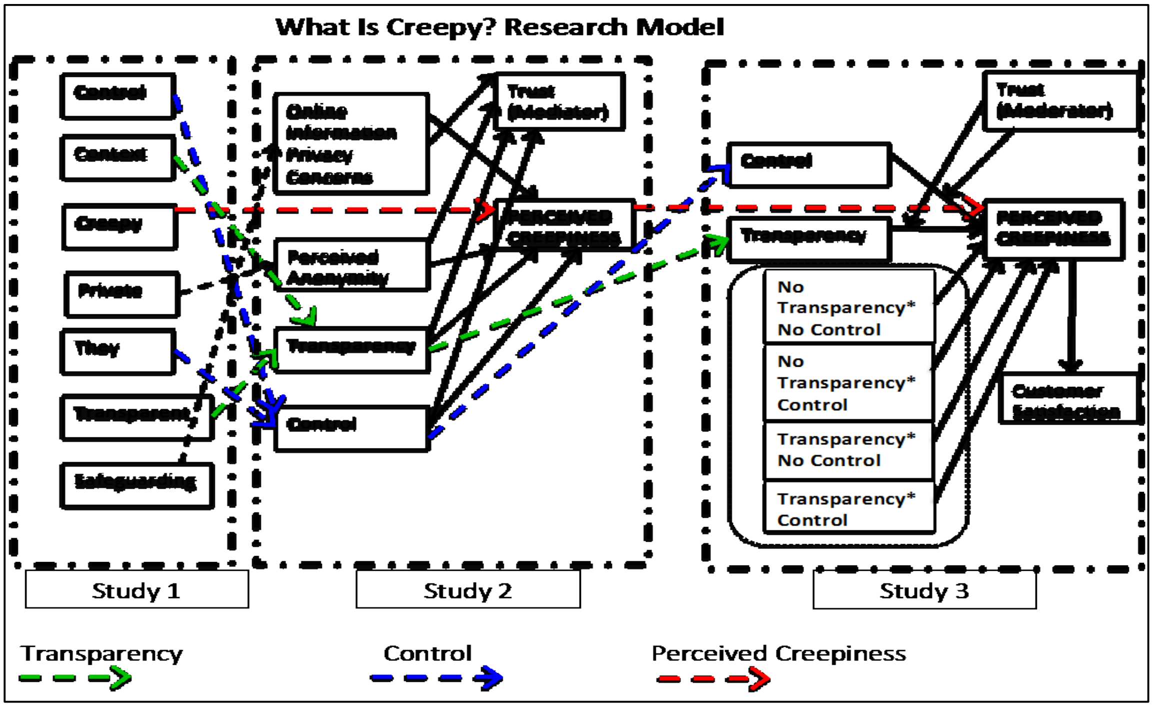
My second study used quantitative methods to test the findings from study one and found online information privacy concerns, transparency and control to be significant factors leading to perceived creepiness. Finally, in the third study, I conducted consumer behavior experiments to determine if consumers' actual behaviors and decisions supported what I found in study two.

Aside from developing a definition of creepy, from these three studies, I concluded that transparency by the firm of their data collection, use and sharing practices so that consumers perceive that they have control over their personal data are key factors that impact perceived creepiness. The degree to which the message is determined to be within or out of context also impacts perceptions of creepiness. Additionally, I found that consumer–firm trust helps to minimize perceived creepiness, and overall perceptions of creepiness have a negative impact on customer satisfaction with the firm.

Research Model

The overall research model is shown in Figure 2. It depicts how the findings of Study 1 lead to the conceptual model in Study 2 and how the results of Study 2 set the foundation for the research model in Study 3. Additionally, it depicts the relatedness of the dominant themes of transparency and control across the three studies.

Figure 2. Research Model



The specific research questions, hypotheses, detailed results, and findings are provided in Chapter 4.

Significance of the Studies

These three studies enabled me to formulate a definition of creepy, develop and validate the perceived creepiness scale to measure perceived creepiness, identify the factors that may lead to perceived creepiness and further test those factors using the perceived creepiness scale. Finally, I was able to measure how personalized messages that were perceived to be creepy can impact the overall satisfaction that a consumer has with a company. The findings from this research not only inform scholarly literature by providing a unified definition of creepy and a scale to measure it and by establishing a theoretical framework toward a Theory of Perceived Creepiness (TPC). They also provide practitioners with knowledge of and directions for navigating the sea of data analytics so that it results in personalized messages that do not produce unsettling feelings and do provide the value that personalized messages can bring (Xu, Dinev, Smith, & Hart, 2011).

The remainder of this dissertation is as follows: Chapter 2 discusses the literature that underpins the three studies; Chapter 3 explains the research design and methods used in the three studies; Chapter 4 presents an overview of the research results and findings from the three studies; Chapter 5 integrates the three studies along with their implications, from a scholarly and practitioner perspective; and Chapter 6 discusses the limitations and provides suggestions for future research. The full research papers for studies one, two and three are in appendices A, B, and C, respectively.

CHAPTER 2: LITERATURE REVIEW

This chapter provides an overview of the constructs, frameworks and theories underpinning my overall research on perceived creepiness. For each study, a literature review was carried out that identified key constructs and theories specific to that study and the particular research questions it addressed. Details can be found in the literature review section of each study (see Appendices A, B, and C).

Academic literature on perceived creepiness is minimal. In surveying the literature, there was no single theory or framework that systematically defined and explained perceived creepiness. Therefore, I followed an inter-disciplinary approach and examined the literature and key theories in the areas of privacy, communication, marketing and information systems (IS). Each discipline provided ideas to explore, from which I went back to the data to determine if what was being explained in theory was actually apparent in the data as well as in practice. Thus, the overall research effort could be thought of as a mixed method grounded theory (Strauss & Corbin, 1998) inquiry, in that existing theories were not focused on the understanding of perceived creepiness, but instead formed a sensitizing device to understanding the data and findings as they emerged.

To begin the literature review, I first searched for research specific to perceived creepiness in the context of personalized marketing messages. I began my dissertation research in 2012, and at that time found one scholarly article that mentioned creepy in a similar context, “Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising” (Ur et al., 2012). It used semi-structured interviews with forty-eight non-technical users to assess their attitudes about and understanding of online behavior advertising (OBA). The respondents feelings about OBA were context dependent and complex in that they felt the ads were both useful and privacy invasive at the same time, which explains the unusual title of the article: Smart, Useful, Scary, Creepy (Ur et al., 2012). The interviewees also expressed concern about the collection of their personal data as the basis for OBA. Although the study mentioned creepy as a feeling respondents have about OBA, it did not define creepiness or the factors that may lead to perceived creepiness, since that was not their focus. Instead, they were interested in describing consumer reactions to OBA. Their study provided insight into the feelings people have about OBA and personalized communication. More importantly, it helped to legitimize the study of perceived creepiness as a real reaction to personalized communication and not just a word haphazardly thrown around about a far-fetched phenomenon.

The next year, another study of creepiness was published by Tene and Polontesky (2013) entitled “A Theory of Creepy: Technology, Privacy and Shifting Social Norms”. In that article, the authors introduce the notion of creepy and identify the conditions under which consumers are most likely to experience creepy: deployment of new technology, new use of existing technology, implementing a feature that eliminates obscurity, unexpected data use or customization. Tene and Polonetsky (2013) state that creepy behavior “leans in” against social norms. The focus of their paper was to provide social as well as legal perspectives that would help consumers, businesses, engineers and lawmakers understand new technologies and ever-changing social norms. They also highlight the subjective nature of creepy and the role of society and social norms in establishing what is perceived to be cool and acceptable versus what is perceived to be creepy. In the final section of their paper, the authors provide strategies to help companies avoid being creepy. Of the strategies they provide, one involves the company being transparent about their data practices. They propose, but do not test, a claim that if companies are more transparent then users may be less surprised or intimidated by certain types of advertisements (Tene & Polonetsky, 2013). Although the article proposes some conditions under which creepiness may emerge, it does not explicitly define creepy nor the specific factors that actually lead to perceived creepiness.

Barnard (2014) explore creepiness and its effect on consumer purchase intention in the study, "The Cost of Creepiness: How Online Behavioral Advertising Affects Consumer Purchase Intention." In Barnard's (2014) study, creepiness is defined as "the sense that marketers are watching, tracking, following, assessing, and capitalizing on an individual's personal information or online activities that she perceived as private" (p. 6). Although the author (Barnard, 2014) identifies conditions which are associated with creepiness, creepy in and of itself is not defined as an emotion or perception by the message recipient. Instead, the author treats it as the set of activities carried out by marketers or online firms. The author states that the creepiness factor occurs when the data used about the consumer is "too personal, too private, too identifiable and too well known" (Barnard, 2014: 6). The study also examined the relationship between the type of information (demographic) used to tailor an ad and the subsequent purchase intentions for a specific product, using reactance theory to underpin the study (Barnard, 2014). The purpose of the study was to conceptualize and operationalize the idea of creepiness in the context of tailored online advertising. The study is similar to my inquiry in that they look at the creepiness factor in the context of tailored communications. However, the author does not identify specific factors that lead to perceived creepiness or provide ways in which marketers and firms can minimize perceptions of creepiness. Through her quantitative study, the author does identify an outcome of the creepiness factor and conclude that creepy tailored communications reduced purchase intentions by five percent, translating into a real cost to companies.

Another recent study related to creepiness is “Creepy Marketing: Three Dimensions of Perceived Excessive Online Privacy Violation” (Moore et al., 2015). This is a qualitative, exploratory study where the authors interviewed 273 college students from a large U.S. public university in the South about what the authors call, Creepy Marketing (CM). In this study, they discuss the impacts of personalized marketing on consumers and then differentiate between “annoying marketing,” which they define as tactics, and “creepy marketing,” which they define as feelings. The interviewees were asked six questions: three pertaining to annoying marketing and three pertaining to creepy marketing. For CM, the responses were categorized into four categories for which they also use to define CM: 1) invasive tactics; 2) causing consumer discomfort; 3) violates social norms; and 4) out of the ordinary tactics. The authors reported that 87% of the responses fell into the categories of invasive tactics, consumer discomfort and violation of social norms. It is from these three categories that they develop the three dimensions of creepy marketing. Their study has some similarities to this work in that they explore creepiness in the context of online communication and equate CM to a feeling of discomfort that is invasive. However, they do not indicate specific factors that lead to CM and do not develop a way to measure the dimensions of CM or define the consequences of CM for the marketer or the firm.

The studies on creepiness in the literature are like pieces of a puzzle. Each one makes a different contribution to our understanding of perceived creepiness. They provide examples of when *creepy* occurs and the conditions for creepy to occur, but none of the studies, by themselves provide a holistic construct of perceived creepiness. My mixed methods study allows me to do exploratory research into a new construct similar to Moore et al. (2015), and to define perceived creepiness in a way that covers all aspects that the previous creepy studies suggest, along with the antecedents and outcomes of perceived creepiness. It also develops a scale to measure perceived creepiness. Therefore, my research fills gaps in the existing literature about creepiness by providing a means to unify the various components of the creepiness studies into a theoretical framework that sets the foundation for a Theory of Perceived Creepiness (TPC). In addition, it operationalizes the construct by defining it, identifying the factors that lead to creepiness and validate a scale with which to measure it.

Two dominant themes that were apparent in my research and were either implicitly or explicitly discussed in the other studies on creepiness were transparency and control. Although the idea of context was briefly alluded to in my first two studies, it emerged as key concept in the third study. Other key themes that emerged from my study centered on data or informational privacy and online information privacy concerns. Without a theory of perceived creepiness to guide my research, these constructs helped me to look inductively at the extant literature to confirm and understand what was occurring in my data. A brief discussion of the key constructs follow.

Privacy

There are many facets of privacy. My study centers on data or information privacy as it specifically refers to the collection and use of personal information. I anticipated that existing privacy theories and online information privacy concern frameworks would provide a lens to interpret the data and findings from my exploratory study and be an entry into my understanding of perceived creepiness, as people would react in a similar manner to an unsolicited message that they perceive to be creepy as they would to an ad or message that they felt was privacy intrusive. Anecdotal evidence showed that perceptions of creepiness of personalized messages felt intrusive and to some degree a violation of privacy. A study conducted by Morimoto and Macias (2009) in which they tested perceived intrusiveness of unsolicited commercial email and its effect on advertising as well as privacy concerns found that the more a consumer found the email to be intrusive, the stronger their reaction would be against it and the more likely they were to have negative attitudes toward it.

In the seminal work of Warren and Brandeis (1890), they state that individuals have a right to privacy and freedom from other intrusions to privacy (Bratman, 2001). Although this assertion does not explicitly address perceived creepiness, it can, however, be extended to Internet activity and applicable to unsolicited personalized messages, targeted pop-up ads and addressing the expectation that some consumers have to not be intruded upon by unsolicited personalized messages while online (Milne, Rohm, & Bahl, 2004; Rohm & Milne, 2004; Sheehan & Hoy, 1999a). Additionally, this framework can apply to the ads that seem to “follow” you on the Internet and appear when it is least expected or wanted.

Online Information Privacy Concerns

Consumers’ concern for privacy impact their behaviors while online in some capacity; often protecting the amount of information they disclose and the degree to which they engage with online companies (Dinev, Hart, & Mullen, 2008). Several frameworks have been developed to help measure Internet users information privacy concerns: the scale of Concern of Information Privacy (CFIP) (Smith, Milberg, & Burke, 1996); Internet Users Information Privacy Concerns (IUIPC) (Malhotra, Kim, & Agarwal, 2004) which is an adaptation of CFIP, and finally Mobile Users’ Information Privacy Concerns (MUIPC) (Xu, Gupta, Rosson, & Carroll, 2012). The purpose of CFIP was to reflect individuals’ concern about organizational privacy practices; the purpose of IUIPC was to communicate Internet users’ concern for information privacy and MUIPC reflected mobile users’ concern for information privacy. Although each has a slightly different focus, all frameworks deal with the most common information privacy concerns: collection, use, transparency, and control. Since consumers’ concern about information affects their online behaviors, those same concerns for privacy impact the emotions that are triggered when the information that they have disclosed has been used in an unsuspecting manner to deliver personalized communications and tailored customer experiences that are perceived to be creepy.

Control

Control not only plays a vital role in defining privacy (Culnan, 1993; Westin, 1966), it also provides a means to understanding perceived creepiness. Having control over how one’s personal information is collected and used is a common theme when it comes to an individual’s personal data and their privacy. Having the ability to control what information is shared, with whom, and under what circumstances, is paramount in maintaining privacy and safeguarding one's personal information. Sheehan and Hoy (2000) suggest that privacy concerns decrease as control over information (collection and use practices) increases. Nowak and Phelps (Nowak & Phelps, 1992) suggest that consumers have little control over what happens after their data is collected and would welcome the opportunity to have more control over the collection and use of their personal information (Phelps, Nowak, & Ferrell, 2000). However, when online, the consumer has minimal control over the collection, use and sharing of their data because of various tracking and monitoring tools that are in place to capture consumer behavior often without their knowledge as well as the inability to opt out of such practices. According to a recent survey, 37% of people expressed that a key concern for them is companies collecting and sharing their data with other companies (TRUSTe/National Cyber Security Alliance, 2016). For consumers who perceive that they have no control over how their information is collected and used to deliver personalized messages they are more inclined to feel vulnerable (Taylor, Davis, & Jillapalli, 2009) and we contend, more susceptible to perceptions of creepiness. As unintended uses of data are more prevalent when the consumer loses control over how their data is collected and used, perceptions of creepiness are more likely to occur when personal information is unknowingly used to create personalized communications. Conversely, as consumers have control over the collection and use of their personal information that they have self-disclosed, they will be less inclined to be "creeped out" because they will know what personal information they have disclosed, to whom and, specifically what and how the information will be used and shared.

Within the privacy domain, the Control and Limitation theories are perhaps the most pertinent to personalized communications or advertisements as it deals with the control an individual has over the collection, use, and sharing of their personal information. Control theories of privacy have a basic premise that one has privacy if and only if one has control over information about oneself (Beardsley, 1971; Fried, 1990; Miller, 1971; Rachels, 1975; Westin, 1968). Control as to how personal information is collected is another determinant that impacts individuals' attitudes and perspectives about information privacy (Culnan, 1993). Even though consumers express trepidation about their privacy while online, Metzger (2007) suggests that consumers' primary privacy concerns in electronic transactions are a result of a consumers' loss of control over their personal information. Control is a dominant and recurring theme as it pertains to information and data privacy and even in defining privacy (Goodwin, 1991). Within the context of marketing and personalized communication, advertisements and tailored customer experiences, privacy exists when a consumer can control the flow of information about themselves. Conversely, it has been suggested that privacy is violated when control is lost (Culnan, 1993; Milne & Gordon, 1993; Simitis, 1987). Further, research has shown that consumers want more control over the collection and use of their personal information (Phelps et al., 2000).

Although this literature views control in the context of privacy, I contend that these same views can be associated with perceived creepiness as well. I suggest that perceptions of creepiness manifest when it appears as if the company "knows" something about the consumer that they did not willingly and knowingly share and had no idea that the company had this information until they received the personalized message (Sheehan, 2002). The consumer has no control over how their data is collected, used and shared, nor do they have the option of opting out of receiving future personalized messages that they perceive to be creepy. If a consumer perceives that they have control over the collection and use of their information, then they may be least likely to be surprised or “creeped out” by a personalized communication or advertisement from a marketer because they have previously disclosed personal information to the marketer or online company.

Transparency

Transparency is a word and concept that is difficult to define as it has varied meanings in different situations or conditions. It is most often seen as a concept relating to compliance or even social responsibility. It has been widely studied across multiple disciplines with each providing a slightly different lens as to what transparency is and how it is operationalized. Although several authors (Dapko, 2012: 1; Eggert & Helm, 2003) have defined transparency, extant academic and practitioner literature do not provide a unified definition. Schnackenberg and Tomlinson (2014) define transparency as the “perceived quality of intentionally shared information from a sender” (p. 5). Further, they suggest that transparency is not a one-dimensional construct as others have suggested, but that it is multi-dimensional and consists of three specific dimensions of transparency: information disclosure, clarity and accuracy.

When discussing Internet Users Privacy Information Concerns (IUPIC), transparency is referred to as awareness (Malhotra et al., 2004). According to Malhotra et al. (2004), within the IUPIC framework, awareness is having an understanding of data collection and use practices of an organization. Further, it refers to “the degree to which a consumer is concerned about his/her awareness of organizational information practices”

(Culnan, 1995; Foxman & Kilcoyne, 1993; Malhotra et al., 2004: 339). However, at the core of its many definitions, transparency is about sharing information in a manner that is perceived to be open and honest about the actions it takes and for the receiver of the information to have full access to the information that they want (Gebler, 2012). If a consumer has an awareness of more than the overall data usage policies of a company, and that company has informed the consumer what information is being collected, how the information will be used and why, then the consumer's need for transparency may be met (Martin, Stadler, Frischmuth, & Lehmann, 2014).. At every step of the information lifecycle—acquiring, processing, storing, disseminating and using (Mason, Mason, & Culnan, 1995: 7)—there is an opportunity for data companies to be forthright about how they handle the information. It has been stated, "the advertising community has been woefully unforthcoming about how much data that they're collecting and what they're doing with it.[8]

Context

According to the New American Oxford Dictionary (2016), context is defined as "the parts of something written or spoken that immediately precede and follow a word or passage to clarify its meaning" (New Oxford American Dictionary, 2016). Thus, a communication is considered to be "in context" when "considered together with the surrounding words or circumstances and "out of context" when the reverse is true. The concept of context is fully embodied by the theory of contextual integrity as defined by Nissenbaum (2009). According to Nissenbaum, contexts "are structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or

[8] (www.cmo.com/bigdataethics/4/3/2014)

rules), and internal values (goals, ends, purposes) (Nissenbaum, 2009: 132). Within this framework, there are norms that govern the flow of information (data) between actors (sender and receiver) centered around transmission—terms and conditions under which data transfer should or should not occur; communication—type of information such as particular data fields; as well as transfer, distribution and dissemination. Collectively, Nissenbaum (2009) refers to this as context-relative information norms (CRIN); it is further stated that contextual integrity is respected when these norms are respected and adhered to, and violated when the information norms are breached. For example, there are norms in place when sharing information with your physician. One expects to share information about their condition; however, they would not expect the physician to discuss or share any medical issues that they may be experiencing with you when you are the patient. If the physician did share information with you, it would violate information norms and "out of context", which could lead to perceptions of creepiness. Additionally, you expect that the information will be only be shared with those that need to know, such as a specialist or others that may tend to your care and to a limited degree with the insurance company. I apply the theory of contextual integrity or context to online personalized messages. In fact, context is an important factor as to whether a personalized message is perceived to be creepy. One may expect that the grocery store to provide relevant coupons based on prior purchases, however, a possible violation or "out of context" situation could occur, if the grocery store provided you with a coupon for a store or for an unrelated grocery item related to something that you may have searched for on the Internet. I suppose that this might be perceived to be somewhat "creepy".

Other Concepts

As previously stated, understanding perceived creepiness requires an interdisciplinary approach. Three other theories and frameworks that helped me to better understand perceived creepiness are 1) Communication Privacy Management (CPM) (Petronio & Durham, 2008, Petronio, 2010) which is a rule-based theory that establishes boundary settings and boundary coordination for effective communication, whereby a violation of a boundary condition creates turbulence. When turbulence occurs, individuals' privacy concerns increase. I posit that a personalized communication perceived to be creepy would qualify as boundary turbulence as it violates boundary rules. Although this theory was initially used to explain communication within interpersonal relationships, the theory can be extended to Internet activity as individuals apply boundary rules and conditions when disclosing personal information online (Metzger, 2007). Further, CPM helps to explain how one can perceive a communication to be creepy or a violation of privacy because of the belief that they no longer have control over their personal information and how it is collected and used (boundary coordination rules). 2) Fair Information Practice Principles (FIPPs), a guiding framework to enhance privacy while conducting online transactions and addresses the privacy of information about individuals (Gellman, 2014) also helps in our understanding of perceived creepiness. FIPPs are concepts that can apply to the electronic marketplace and provide a means in which to operationalize procedural fairness. 3) Social Contract Theory (SCT) (Friend, 2004; Rawls, 1999) which is an implied agreement between an individual and the firm with whom they share their personal information. SCT posits that consumers and marketers enter into an implied, (for which they do not have a choice), social contract when they willingly exchange their personal information and negative feelings for something of value, such as access to a website or to obtain discounts (Dunfee, Smith, & Ross Jr., 1999; Friend, 2004). Related to SCT is procedural fairness. Procedural fairness is the perception by a consumer that an interaction in which they were a part was conducted fairly (Lind & Tyler, 1988) Factors that contribute to procedural fairness include voice and control (Folger & Greenberg, 1985; Lind & Tyler, 1988). If the consumer perceives that they are being treated fairly, then it is possible that perceptions of creepiness are minimized.

Embedded in these frameworks are the themes of transparency and control. For example, transparency is the first principle of the Fair Information Practice Principles (FIPPs), which ensures no secret data collection and provides information about the collection of personal data to allow users to make an informed choice (Culnan & Armstrong, 1999) and a lack of transparency may be perceived as a breach of the Social Contract that is implicit between the firm and the consumer.

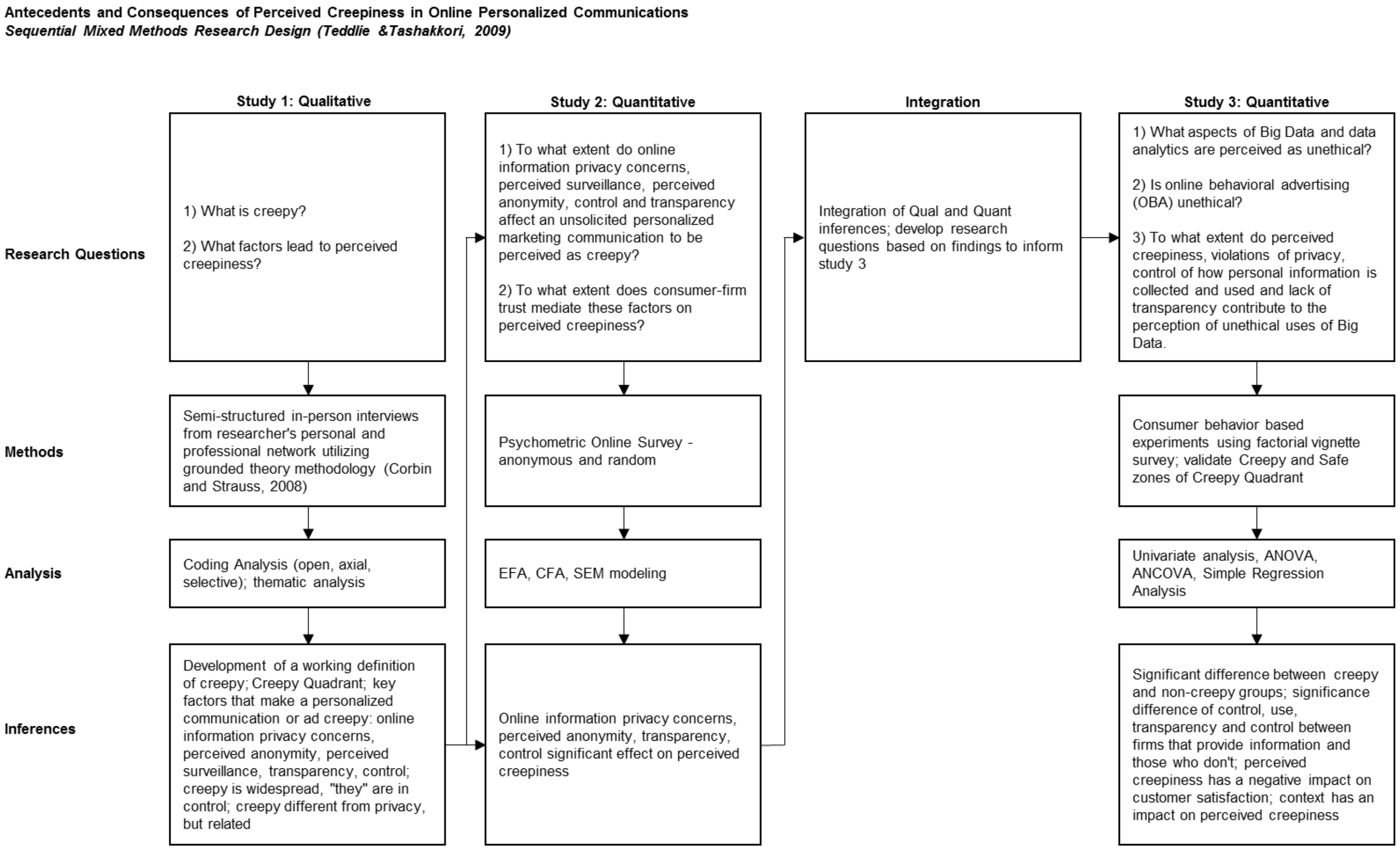
I included two ancillary constructs, consumer–firm trust and customer satisfaction to help in understanding the impacts of perceived creepiness. Even though they were not central to its definition or to identifying the antecedents of perceived creepiness, they were relevant to understanding the outcomes or consequences of delivering personalized communication that is perceived to be creepy. Detailed information about these constructs are found in the studies to which they apply: consumer–firm trust—studies two and three, (see Appendices B and C) and customer satisfaction—study three (see Appendix C). My inter-disciplinary literature review reflects the relatedness of my study's themes across multiple disciplines, confirming that perceived creepiness is a complex phenomenon in need of a unified or holistic framework in order to more fully comprehend it.

CHAPTER 3: RESEARCH DESIGN & METHODS

To understand the antecedents and consequences of perceived creepiness, I employed a sequential, mixed methods design (Creswell & Plano Clark, 2011; Teddlie & Tashakkori, 2009). My dissertation is comprised of three distinct strands: QUAL→Quant→Quant (Creswell, 2003). The use of a mixed methods approach allowed me to develop a more pragmatic perspective that neither a qualitative study nor a quantitative study alone would provide. Utilizing a mixed methods approach was most appropriate for my study because it allowed for exploratory research about individuals' perspectives of perceived creepiness and then builds upon those insights to obtain a deeper understanding of perceived creepiness. The entire dissertation is based on grounded theory (Charmaz, 2006a; Glaser & Strauss, 1967; Strauss & Corbin, 1998) methodology in which I interpret the data and identify key themes from one study to inform the inquiry of the next study. Thus, my overall study is a sequentially deeper inquiry into the creepy phenomena.

The integrated research design (Figure 3) shows an overview of my mixed methods study along with the integration points for each study. The findings from each study provided the basis for the subsequent study and built on those findings.

Figure 3. Integrated Research Design



Antecedents and Consequences of Perceived Creepiness in Online Personalized Communications
Sequential Mixed Methods Research Design (Teddlie &Tashakkori, 2009)

	Study 1: Qualitative	Study 2: Quantitative	Integration	Study 3: Quantitative
Research Questions	1) What is creepy? 2) What factors lead to perceived creepiness?	1) To what extent do online information privacy concerns, perceived surveillance, perceived anonymity, control and transparency affect an unsolicited personalized marketing communication to be perceived as creepy? 2) To what extent does consumer-firm trust mediate these factors on perceived creepiness?	Integration of Qual and Quant inferences; develop research questions based on findings to inform study 3	1) What aspects of Big Data and data analytics are perceived as unethical? 2) Is online behavioral advertising (OBA) unethical? 3) To what extent do perceived creepiness, violations of privacy, control of how personal information is collected and used and lack of transparency contribute to the perception of unethical uses of Big Data.
Methods	Semi-structured in-person interviews from researcher's personal and professional network utilizing grounded theory methodology (Corbin and Strauss, 2008)	Psychometric Online Survey - anonymous and random		Consumer behavior based experiments using factorial vignette survey; validate Creepy and Safe zones of Creepy Quadrant
Analysis	Coding Analysis (open, axial, selective); thematic analysis	EFA, CFA, SEM modeling		Univariate analysis, ANOVA, ANCOVA, Simple Regression Analysis
Inferences	Development of a working definition of creepy; Creepy Quadrant; key factors that make a personalized communication or ad creepy: online information privacy concerns, perceived anonymity, perceived surveillance, transparency, control; creepy is widespread, "they" are in control; creepy different from privacy, but related	Online information privacy concerns, perceived anonymity, transparency, control significant effect on perceived creepiness		Significant difference between creepy and non-creepy groups; significance difference of control, use, transparency and control between firms that provide information and those who don't; perceived creepiness has a negative impact on customer satisfaction; context has an impact on perceived creepiness

I begin my mixed methods research with a qualitative study because qualitative methods lend themselves to more inductive and exploratory research. This approach allowed me to thoroughly explore and identify emergent themes and additional constructs pertaining to perceived creepiness. In my qualitative study (Appendix A), I utilized Grounded Theory methodology initially proposed by Glaser and Strauss (1967) as refined by Strauss and Corbin (1998) and Charmaz (2006a). Grounded theory emphasizes the understanding of human behavior by developing theories of it based on data collected through interviews with and observations of people. Because I am trying to understand how people experience personalized communications and their reactions or feelings toward them, grounded theory methodology was best suited to gain insight about those lived experiences. I conducted semi-structured interviews with a small (22 people) convenience, purposive sample recruited from my personal and professional network. The interview protocol consisted of approximately sixteen questions centered on the participants experience with online communication and advertisements and how these communications made them feel.

My second study was a quantitative inquiry to test whether the findings from my qualitative study were generalizable to a larger sample. Prior to testing the identified themes, I had to develop a scale to measure perceived creepiness, because there were no scales that could be used to adequately measure that construct. To aid in my development of the scale, I referenced the works of Churchill (1979), Hinkin (1995), and Mackenzie et al. (2011). I adopted the 10-step process of developing constructs for MIS and behavioral research as stated by Mackenzie et al. (2011). To measure perceived creepiness, I developed an 8-item scale known as the Perceived Creepiness scale. See Appendix D for details on its development.

For this quantitative study, I used a random sampling of subjects to complete a validated online psychometric survey (Guilford, Christensen, & Bond, 1954) which links individual responses to the constructs within my research model. The questions addressed online privacy concerns, transparency, perceived surveillance, perceived anonymity, control, and trust. Of the twenty-one questions, eight were directly related to my constructs along with three scenarios in which the respondents were to assess the degree of perceived creepiness; six questions concerned Internet usage and activities performed using the Internet, and three demographic questions were asked about age, gender and highest educational level obtained and one question to address Common Method Bias (CMB). Since I measured the independent and dependent variables within the same instrument, it was necessary to assess Common Method Bias. To do so, I used a social desirability scale (Hays, Hayashi, & Stewart, 1989) assuming that there is a socially desirable way to answer questions about perceptions, emotions, and beliefs. Many of the constructs in my model, especially perceived creepiness, are predicated on a person's emotions, perceptions, and mental models. The survey was sent to my professional and personal network, and posted on social media sites, including Facebook, LinkedIn and Amazon's Mechanical Turk (MTurk).[9] This first quantitative study (Appendix B) was

[9] Mechanical Turk is an Internet crowdsourcing marketplace where requestors post jobs to complete called a HIT (human intelligence task) and workers choose the HIT's to complete for a small fee. Mechanical Turk has increased in popularity and usage among Social Science researchers because of its ability to get high quality data rapidly and inexpensively (Buhrmester, Kwang, & Samuel D Gosling, 2011). One of the benefits of Mechanical Turk is the diversity of the respondents, which (Buhrmester, Kwang, & Samuel D. Gosling, 2011) found to be more diverse than college students who are often used in research studies.

confirmatory of the initial qualitative study. By combining a quantitative study with a prior qualitative study, I was able to more accurately measure the effects of various factors that may be antecedents to perceived creepiness. The quantitative study enabled me to measure the extent to which the factors that were identified in my qualitative Study 1 (Appendix A): Online Information Privacy Concerns, Perceived Anonymity, Perceived Surveillance, Transparency (Firm) and Control (Consumer) contribute to a personalized communication being perceived as creepy. Additionally, following the qualitative study with a quantitative inquiry allowed me to test the inferences I made from the qualitative study using a hypothetico-deductive model (Tashakkori & Teddlie, 2010; Teddlie & Tashakkori, 2009). The combined results and findings from those two initial studies informed Study 3, a behavioral experiment quantitative study (Appendix C).

Study 3 was also a confirmatory study where I conducted consumer behavior experiments to confirm that transparency and control are antecedents of perceived creepiness. In my first study, transparency and control were themes that emerged from the interview data and from which the Creepy Quadrant (Figure 1) was created. In the second study, the hypothesis was supported that transparency and control are factors that had a negative effect on perceived creepiness. The purpose of my third study was to validate the Creepy Quadrant (Figure 1), which shows the interaction between transparency and control and how the combination of the two factors leads a personalized message to be perceived as creepy in the Creepy Zone or the Safe Zone where the message is not perceived to be creepy.

One method often used in marketing research to assess consumer behavior are experiments using factorial vignette survey methodology (Jasso, 2006), which I used in the final quantitative study. Vignettes are short hypothetical stories in either written or pictorial form in which respondents can provide comments usually with survey type questions (Renold, 2002). Hughes states that vignettes are "stories about individuals, situations and structures which make reference to important points in the study of perceptions, beliefs and attitudes" (Hughes, 1998, p. 381). Factorial surveys begin with a selection of variables describing the situation, in my study, personalized communications followed by questions varying the dimensions of transparency, control, trust, context, data collection, use, and sharing. According to Auspurg, Hinz, and Liebig (2009), by varying the causal effects of the various dimensions the researcher is able to test the respondents' reaction. Vignettes are most appropriate for capturing societal norms and attitudes about specific situations. Factorial vignette methodology is also designed to identify normative judgments, which are dependent on contextual factors that can be used to examine various elements of information on which judgments are based (Martin, 2012). Using factorial vignette surveys makes it possible to ascertain the relative weights of a single variable that describes a situation while simultaneously examining multiple factors (Auspurg et al., 2009; Jasso, 2006) and also to see how different groups may respond to the scenarios (Martin, 2012). Additionally, utilizing this method, researchers have the ability to try and understand what the respondent is thinking about and their judgments of complex constructs. Perceived creepiness is a complex construct due to its subjective nature, and there could be a number of factors that may lead to perceived creepiness. Using factorial vignettes helped me to tease this out. Some have suggested that vignette analysis can yield an exact measurement of attitudes (Hechter, Kim, & Baer, 2005; Jasso, 1988). Auspurg et al. (2009) proclaim that using factorial vignette surveys has several advantages: 1) Vignettes are constructed using a collection of variables; 2) Larger samples can be tested than in traditional experiments; 3) The ability to test between and within factors among the respondents; 4) One can simulate complexities of the real world in more realistic situations that are not one dimensional; and 5) Vignettes are less biased against social desirability.

Since I am seeking to understand perceived creepiness and the factors that cause a personalized communication to be perceived as creepy, this methodology seemed well suited for my research. I was able to vary several factors that were hypothesized to lead to or impact perceived creepiness: transparency, control, context of the message, trust and customer satisfaction. Respondents can be randomly or systematically selected, and in my study, respondents were randomly selected for the specific vignette that they received. This allowed me the opportunity to get a balanced and diverse sample for each condition (vignette). In view of the advantages of using factorial vignette surveys and the ability to simulate the complexity of the real world and cultural norms, this methodology was beneficial in understanding the effects of transparency and control and how it impacts perceived creepiness.

Given the subjectivity of perceived creepiness, the mixed methods design allowed me to triangulate the findings from the QUAL→ Quant→Quant sequence, which helped in identifying and confirming the antecedents and consequences of perceived creepiness. Further, it is the combination of inductive and deductive logics in a mixed methods study (Creswell & Plano Clark, 2011) that allowed me to address the complex research questions and meet the study objectives.

CHAPTER 4: STUDY RESULTS

The findings from my research are relevant because the term “creepy” is used quite often to describe marketing communications as well as technology that are unsettling. The subjective nature of the term lends itself to multiple interpretations, so having a unified definition of creepy and an understanding of the factors which lead to perceiving a personalized communication as creepy helps to uncover what is *really* meant when it is stated that a particular communication or customer experience is perceived to be creepy. Further, the findings will help to inform marketers and online firms what they should or should not be doing in order to avoid sending personalized messages that are perceived to be creepy. An overview of the findings from the three studies follows.

Study 1: What is Creepy? Towards Understanding That Eerie Feeling When it Seems the Internet “Knows” You

The first study was a qualitative inquiry to explore perceived creepiness. The primary goal of this initial study was to develop a definition of creepy and identify factors that lead to a personalized message to be perceived as creepy. The specific research questions I sought to address were: 1) What is creepy? and 2) What factors lead to perceived creepiness? In an attempt to answer these questions, I interviewed 22 individuals from 18 to 64 years old, 59% female, about their experience of personalized online communications. When using grounded theory (Charmaz, 2006; Glaser & Strauss, 1967; Strauss & Corbin, 1998) methodology, the researcher allows the data to “speak” from which conjectures emerge. The interview data enabled me to define perceived creepiness and identify factors, which seem to stimulate, or be antecedents of, perceived creepiness.

Key Findings & Outcomes

The twenty-two semi-structured interviews generated 1,356 segments of text to code, from which 279 codes were generated, falling into 50 broad categories, from which seven themes became apparent (Control, Context, Creepy, Private, THEY, Transparency and Safeguarding). The interview data was insightful as I was able to establish a definition of creepy and identify factors that may lead to perceived creepiness. Additionally, there were other key findings that emerged from this study: 1) The feeling or experience of creepy from a personalized communication or ad is widespread; 2) Creepy and Privacy Intrusive are related, but different; 3) "THEY" are in control; and 4) Lack of control as to how personal information is used online led to safeguarding and protecting private or personal information even though the individual claimed that they had "nothing to hide."

The definition of creepy that emerged from the qualitative study is: an emotional reaction to an experience, interaction, technology or unsolicited communication where personal information has been collected with or without your knowledge and used in an unexpected or surprising manner invoking negative feelings. The factors that I found which might contribute to a personalized message being perceived as creepy were: context, online information privacy concerns, perceived anonymity, perceived surveillance, transparency, control, and trust. I expected that the mere presence of these factors does not necessarily invoke the creepy factor and that it is the interplay or conjoining of these factors. I selected two of the most dominant themes: transparency and control to develop the Creepy Quadrant, which is a visual depiction of the interrelationship of transparency and control and how it impacts perceived creepiness (See Figure 1, Chapter 1).

The findings, conclusions, generalizations and outcomes from the qualitative study informed the latter two quantitative studies as well as provided the basis for developing a scale to measure perceived creepiness. Therefore, the qualitative study was the dominant study of the three, as it laid the foundation for my research and formed the basis of my understanding of perceived creepiness of personalized messages. Study 1 in its entirety, which includes details of the findings, is found in Appendix A.

Study 2: Demystifying Creepy Marketing Communications

I then conducted a quantitative study using an online survey to test whether the factors identified in the qualitative study, survey-based study to test whether the factors identified in the first, qualitative study are actual antecedents of perceived creepiness. The primary research question driving the second study was: “To what extent do online privacy concerns, perceived surveillance, transparency, control and perceived anonymity result in a personalized marketing communication being perceived as creepy?” A secondary research question my study addressed was: “To what extent does consumer-firm trust mediate those antecedents of perceived creepiness?” The survey was disseminated via several channels, over a period of four weeks, during which time I collected 389 valid responses (average age = 37 years old; 45% female). I tested the research questions with several hypotheses. Of the factors tested, I found online information privacy concerns, transparency and control to be significant and support my initial hypotheses (Figure 4). These findings form the basis for my next study.

Figure 4. Study 2 Hypotheses

Online Information Privacy Concerns has a positive effect on Perceived Creepiness (0.44, p-value=.001)
Transparency has a negative effect on Perceived Creepiness (-.11, p-value=.008)
Control has a negative effect on Perceived Creepiness (-0.22, p-value=.001)

Key Findings & Outcomes

In this confirmatory study, I used the Perceived Creepiness scale that I developed to confirm whether the factors tested affected or led to perceived creepiness. I was able to validate that online information privacy concerns have a positive effect on perceived creepiness; transparency and control have a negative effect on perceived creepiness, and the other factors tested did not have a significant impact on perceived creepiness. I also found that trust did not have a mediating effect between the exogenous variables and perceived creepiness. From these findings, I conclude that online information privacy concerns, transparency and control are antecedents of perceived creepiness within the context of personalized communications.

Additionally, I conducted a post hoc analysis and analyzed the responses and results from three fictitious scenarios that were developed to ascertain the degree to which they were perceived to be creepy. The scenarios mimicked real world activities that may occur while on the Internet. The data from the scenario responses seem to indicate that: having a relationship with the company does not necessarily change the perception of creepiness. Further, a breach of a social contract occurs when the consumer assumes that the online company will manage and not misuse their personal information but fails to do so. Additionally, perceived creepiness can occur when a seemingly unknown fact appears to be known by a company with whom there was not an established relationship.

I also reviewed responses regarding eight words and one phrase (Good, Smart, Useful, Scary, Creepy, Relevant, Surprising, Evil and Violation of my Privacy) to describe unsolicited personalized marketing communications and advertisements. The top five words in which respondents somewhat agree, agree or strongly agree in describing personalized communications were 1) Violation of privacy (77.90%), 2) Creepy (73.00%), 3) Scary (65.30%), 4) Surprising (43.80%), and 5) Smart (33.00%). This finding supports my premise that personalized messages can be perceived as creepy as well as the definition of creepy as defined in my study, whereby, data is collected in a surprising manner invoking negative feelings. Lastly, I reviewed respondents' Internet usage, safeguarding measures and the most common activities performed on the Internet. From this data, I found that when the respondents were online they typically watched videos (96%), used online mapping services (93%), shopped (93%) read newspapers or magazines (89%) conducted banking (86%) and participated in various types of social media (89%). Surprisingly, only 34% of the respondents clicked on pop-up ads, which in some cases may have been personalized for them based on their digital dossier.

To safeguard personal information or avoid online advertising, respondents refused to provide information to a website because they felt the data being asked was too personal (82%), did not use a website because it was unclear as to how the data would be used (67%) and 55% asked a website not to share their personal information with others.

The purpose in gathering this information was to assess whether the level of Internet experience impacted perceptions of creepiness, and finally, what types of safeguarding measures consumers take to avoid unsolicited personalized communications that may be perceived to be creepy. Study 2, in its entirety, which includes details of the findings, is found in Appendix B.

Study 3: The Effect of Transparency, Control, Control and Trust on Perceived Creepiness of Online Personalized Communications

Transparency and control are themes that have surfaced and have remained apparent throughout studies one and two as antecedents of perceived creepiness of online personalized messages. Because transparency and control continued to be strongly associated with perceived creepiness, I wanted to use a behavioral experiment to validate the Creepy and Safe zones within the Creepy Quadrant and confirm that transparency and control play an important role in perceived creepiness of personalized online communication. The purpose of this final, quantitative study was three-fold: 1) Validate the Creepy and Safe zones within the Creepy Quadrant; 2) Assess the impact of creepy communication on customer satisfaction; and 3) Ascertain the role of trust as it pertains to transparency, control, and perceived creepiness. I addressed the following research question using scenario-based (vignette) (Jasso, 2006) experiments followed by a factorial survey: “How do levels of transparency and control impact perceived creepiness?” In my third study, I also wanted to measure how perceived creepiness of online personalized communications is related to customer satisfaction with the firm, addressing the question: to what extent do creepy personalized messages affect the level of customer satisfaction with a firm? Another important question I wanted to explore was whether message recipients were more likely to perceive messages as being creepy when they involved elements that were “out of context” than when the message was uniformly "in context." The hypotheses guiding study three were supported and found to be significant as shown in Figure 5.

Figure 5. Study 3 Hypotheses

Hypotheses 1: Transparency by the firm will have a negative effect on perceived creepiness (F=122.521, p-value=.000)

Hypotheses 2: Perceived Control by the consumer over the collection, use, and sharing of their data will have a negative effect on perceived creepiness of personalized messages (F=69.496, p-value=.000)

Hypotheses 3: The Creepy Quadrant is an interaction between transparency and control such that:

> **Hypotheses 3a:** No transparency by the firm and no perceived control by the consumer will increase perceptions of creepiness (Creepy Zone) (F=10.380, p-value=.000)
>
> **Hypotheses 3b:** Transparency by the firm and perceived control by the consumer will decrease perceptions of creepiness (Safe Zone) (F=10.380, p-value=.000)

Hypotheses 4: Trust will positively moderate the effects of transparency on perceived creepiness, such that, a high (low) level of trust will decrease (increase) the effects of transparency on perceived creepiness (F=60.753, p-value=.000)

Hypotheses 5: Trust will positively moderate the effects of control on perceived creepiness, such that, a high (low) level of trust will decrease (increase) the effects of perceived control on perceived creepiness (F=60.753, p-value=.000)

Hypotheses 6: Perceived Creepiness will have a negative effect on customer satisfaction (β=-.485, p=<.001)

Key Findings & Outcomes

In this last study of my mixed-methods inquiry on perceived creepiness, I conducted experiments using factorial vignette surveys (Jasso, 2006). In the experiment, the respondents were provided with a situation where they booked a vacation with an online travel company called Vacation Finders, which collected personal information. The respondents were randomly assigned to one of two conditions: provide and not provide. In the "provide" condition, Vacation Finders provided information as to how the consumers' data would be collected, used and shared along with a way to control how their data would be used and shared; in the “not provide” condition, the reverse was true, Vacation Finders did not provide information as to how the consumers’ information would be collected, used and shared nor was there any way to control how this information would be used. In addition to the conditions, the respondents were randomly given one of three email scenarios: 1) from a winery offering wine tours and wine tasting; 2) from a restaurant near where you live offering birthday dinner offers; and 3) your personal contacts were accessed to direct them to send birthday greetings, followed by survey questions measuring perceived creepiness, transparency, control, use, trust and customer satisfaction. From these experiments, I was able to confirm that there is a significant difference among trust, use, transparency, and control when the firm provides information about its data collection, use and sharing practices than when it does not provide the information. Next, I found that perceived creepiness varies between the two conditions (provide/not provide) as well. Personalized communications are perceived to be creepier when information is not provided than when it is provided. Also, perceived creepiness does vary with the content of the message and whether it is “in context” or “out of context”, that is - whether the meaning of the message is “in context” and aligned with the situation or circumstances under which it was sent, or “out of context” and does not align with the current situation (Nissenbaum, 2004). For example, if a restaurant sent you a special offer for a meal reflecting the region of Italy you had just visited on a tour organized by a local travel agent, it would be an “in context” communication. If the same restaurant sent you a “Happy Birthday” greeting, it would be “out of context”.

When combining the effects of the provide/not provide condition with the various scenarios, perceived creepiness was not significantly different when information is provided than when it is not provided. Although I was not able to measure all of the zones within the Creepy Quadrant, I was able to confirm the two extremes: the Creepy Zone where the firm is not transparent and the consumer has no control over their personal information and the Safe Zone where the opposite is true are valid.

I hypothesized that trust would have a moderating effect on perceived creepiness. However, that was not the case; trust had a direct effect on perceived creepiness, meaning when consumers trust the company, perceived creepiness decreases, conversely, when there is low trust for a company, perceived creepiness increases dramatically. Lastly, in terms of customer satisfaction, personalized online communications that are perceived to be creepy do have a negative effect on customer satisfaction, such that, when consumers feel as though the personalized message that they receive is perceived to be creepy, their overall level of satisfaction of the firm decreases. Another measure I used to assess customer satisfaction was the Net Promoter Score (Reichheld, 2003), a measure often used by firms to assess growth, how they measure up against their competitors and customer satisfaction. The NPS asks one question, "How likely are you to recommend (company name)?" which is rated from 1 to 10, with 1 being not likely, and 10 being likely. The responses are categorized as detractors, passives or promoters. In this experiment, the respondents were in the detractors category, meaning the customers are unhappy with Vacation Finders and how they collected, used and shared their personal information.

Study 3, in its entirety, which includes details of the findings, is found in Appendix C.

CHAPTER 5: DISCUSSION

When I embarked on this journey to understand perceived creepiness, my primary research objectives were to determine what does it *really* mean when personalized online communication is described as creepy and also to identify the antecedents and consequences of perceived creepiness. My ultimate goal was to operationalize Perceived Creepiness as a construct by defining it, identifying factors that lead to it and developing a scale to measure it. I was able to triangulate the findings from this mixed methods research and fully integrate the data from all three studies to help in understanding perceived creepiness within the context of personalized messages. The empirical findings of each study[10] contribute to an explanation of how the creepy phenomenon is socially constructed and what is *really* behind the word "creepy". Moreover, I was able to synthesize all of this information to develop a theoretical foundation toward a Theory of Perceived Creepiness (TPC). This research furthers the discussion of creepy, which is in the early stages of being researched as we seek to understand and make sense of the modern world and the data-driven society in which we live.

In order to understand the theoretical framework for perceived creepiness, we must first understand how people engage in sense-making behaviors to explain that which they do not understand. Thus, it is through the lens of structuration and social construction where social norms emerge that helps to inform how we process our environment. It is often said that perception is reality; that which we socially construct is real. Therefore, perceived creepiness is real although we may not be able to precisely

[10] The Discussion section of each study provides details of the findings and the research question and model being researched. The full studies can be found in Appendices A, B, and C.

define it and supports the idea that “I know it when I see it” (Lattman, 2007; Stewart, 1964). One way to make sense of something is by invoking social imaginaries. According to Taylor (2002), social imaginaries embody the ways in which ordinary people imagine their social existence and surroundings, which are seen in images, stories, and legends that people pass along. The social imaginary is shared by large groups of people or even the society. In my qualitative study (Study 1, Appendix A), the respondents did not always say *creepy* when sharing their experiences; however, when they were asked about *creepy,* they had an example. No one needed clarification on what was meant by *creepy*. Taylor (2002) states, “the social imaginary is that common understanding that makes possible common practices and a widely shared sense of legitimacy” (p. 106). This is perhaps why the term is so pervasive in its use, although what the term “creepy” really means has been evasive and somewhat ambiguous.

The process of constructing reality is most often brought about through social interaction. The social construction of reality is a dialectical process in which human beings act both as the creators and as products of their social world (Adoni & Mane, 1984). Within this dialectical process, there are three types of reality: 1) objective social reality, which exists outside of the individual and presented as facts; 2) symbolic social reality, which refers to any form of symbolic expression of objective reality such literature, media or art; and 3) subjective social realities, where both the objective and symbolic realities are inputs for the construction of the individual’s own subjective reality (Adoni & Mane, 1984). It is in this realm of reality where Perceived Creepiness exists. It is indeed subjective, and a multi-dimensional construct as what is creepy to one person may, in fact, be cool to another person. While this is not an exegesis on the philosophical discussion on the social construction of reality (Berger & Luckmann, 1991) or structuration theory (Giddens, 1984), suffice it to say that these sense-making behaviors and mental models influence what is currently perceived to be creepy. Contextual integrity (Nissenbaum, 2009) provides a unique perspective on how violations of informational norms can affect whether a message is perceived as being creepy or not. If the message, in large part, aligns with and respects informational norms, then the message may be more likely to be received favorably. However, if the message is seen as violating informational norms, then it may be more likely to be perceived as creepy. This will be an important part of my study of creepiness.

Given that society socially constructs reality, I wanted this research to push beyond social constructionism and provide empirical evidence supporting the existence of the creepy phenomena and its underpinnings. To that end, my three-study inquiry of perceived creepiness allowed me to do that. Each study in the QUAL→Quant→Quant sequence built on the prior study and I was able to synthesize the emerging findings and develop a theoretical framework to help in understanding the creepy phenomena that previously has not been fully explained, as well as lay a foundation upon which to build a Theory of Perceived Creepiness (TPC). Theory is described as "a coherent description, explanation and representation of observed or experienced phenomena" (Gioia & Pitre, 1990: 587). In order for theory to be of value it should "explain the meaning, nature, and challenges of a phenomenon, often experienced but unexplained in the world in which we live, so that we may use that knowledge and understanding to act in more informed and effective ways" (Lynham, 2002: 222). To build a theory within an applied discipline, such as marketing, and be applicable within the "real world" requires that problems of practice be explored in a comprehensive manner (Swanson & Chermack, 2013). When both practitioners and scholars have a voice in explaining and understanding the phenomena, a more complete and balanced perspective is provided that is sound from a scholarly and academic perspective and equally applicable to everyday life. Theory building is the continuous and recursive process of conceptualization, operationalization, confirmation, application and refinement (Lynham, 2002; Swanson & Chermack, 2013). In the conceptualization phase, the phenomena or problem of practice in presented; in the operationalization phase, the connection between the concept and practice takes place; in the confirmation phase, the theoretical framework is either supported or disconfirmed; in the application phase, the framework is applied within the environment where the phenomena exist and in the refinement phase, the framework is refined and developed as new learnings and applications are discovered (Lynham, 2002).

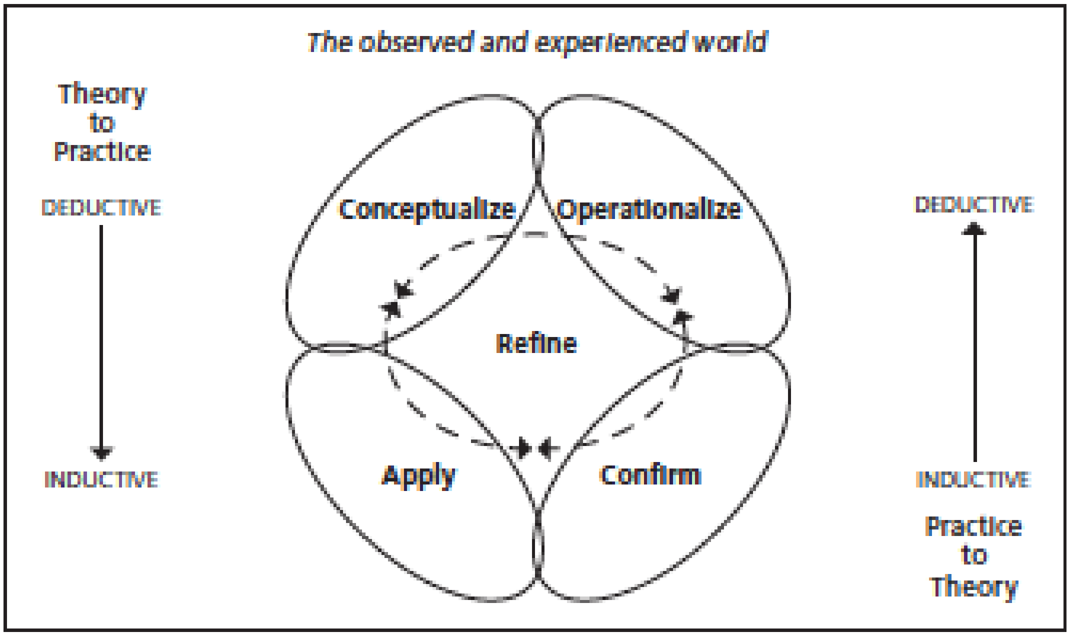
From a theoretical perspective, there is not a unified theory that guides our epistemology of perceived creepiness. Of the studies related to perceived creepiness of personalized marketing messages that I have identified (Barnard, 2014; Moore et al., 2015; Tene & Polonetsky, 2013; Ur et al., 2012), only one proposes a theory of creepiness (Tene & Polonetsky, 2013). Although that study proposes a theory, the focus is on creepiness from technology that “leans in” against traditional social norms (Tene & Polonetsky, 2013). In their study, Moore et al. (2015) do identify dimensions of the creepiness construct but fall short in developing a theory. The other two studies do not make any claims in developing a theory of perceived creepiness.

Building on The General Method of Theory Building in Applied Disciplines (Figure 6) suggested by Lynham (2002) and further developed by Swanson and

Chermack (2013), my study on perceived creepiness provides a theoretical framework on which to build a Theory of Perceived Creepiness (TPC).

Figure 6. General Method of Theory Building in Applied Disciplines

(Swanson & Chermack, 2013)



Source: Adapted from Lynham (2002).

Through this inductive mixed methods (QUAL→Quant→Quant) research, I was able to conceptualize, operationalize, confirm, and apply a framework of perceived creepiness.

Theory Building

Conceptualize – The Phenomenon of Problem of Practice is Presented

I was able to conceptualize the Perceived Creepiness construct by confirming that it is a legitimate emotion and reaction to personalized messages and online behavioral advertising as stated by Ur et al. (2012). Additionally, I highlighted several practitioner articles where marketers are admonished to not be creepy with their personalized ads.

The limited research did not provide a clear and unified definition of creepy; also, the factors that lead to perceived creepiness and what should or should not be done to minimize perceived creepiness had not been clearly defined. The majority of the conceptualization of perceived creepiness had been observed in practice and conducted prior to formally launching my study. The findings from my qualitative study (Study 1) also helped to conceptualize this phenomenon.

Operationalize – The Connection between the Concept and Practice Takes Place

To operationalize the perceived creepiness construct I first defined perceived creepiness based on the findings and insights from my qualitative study.

> Perceived creepiness is an emotional reaction to an experience, interaction, technology or unsolicited communication where personal information has been collected with or without your knowledge and used in an unexpected or surprising manner invoking negative feelings.

Next, I developed a scale to measure perceived creepiness (see Appendix D). Using the Perceived Creepiness scale, I was able to validate the factors that had been identified as leading to perceived creepiness. Additionally, I was able to take two of the dominant themes that first surfaced in Study 1, (transparency and control) and develop the Creepy Quadrant (Figure 1), which is a visual depiction of the interrelationship between those factors. The findings of study two were critical in operationalizing the perceived creepiness construct.

Confirm – The Framework is Applied within the Environment Where the Phenomenon Exists

In order to confirm the construct, I conducted consumer behavioral experiments using factorial vignette surveys (Jasso, 2006) which simulated reality. In that survey, respondents were presented with conditions and scenarios that mimicked reality and personalized communications that were creepy. The results from Study 3 confirm that perceived creepiness is a valid construct and that there are distinct differences between online personalized communications that are perceived to be creepy when transparency and control are not provided, shown as the Creepy Zone in the Creepy Quadrant (Figure 1) and where transparency and control are provided, shown as the Safe Zone (Figure 1).

Apply – The Theoretical Framework is Either Confirmed or Disconfirmed

In Study 3, I attempted to apply the construct by measuring the impacts of online personalized messages that are perceived to be creepy and the extent to which customer satisfaction is affected. Although this experiment validated the perceived creepiness construct, more research is needed to apply the framework in various situations and other contexts where perceived creepiness may exist.

Refine – The Framework is Refined and Developed as New Learnings and Applications are Discovered

More research needs to be conducted using the Perceived Creepiness scale and theoretical framework so that additional insights are learned and more empirical evidence of the framework being applied is available; after which, it will be more plausible to fully adopt the theoretical framework into a valid Theory of Perceived Creepiness.

Implications for Scholars

Perceived creepiness as it pertains to personalized communication, marketing tactics and technology is a term often used by practitioners, without a clear definition and a myriad of interpretations and hence, in the early stages of being researched in academic literature. With this dissertation research, there is an opportunity to contribute to a growing body of literature on a phenomenon that has been under-researched and enter into a conversation that is only beginning. There is also the chance to contribute to the discussion of consumer reaction to online behavioral advertising and receiving unsolicited personalized messages. This mixed-method study has helped to bring an increased awareness of perceived creepiness especially within the context of personalized communication. The Creepy Quadrant also adds to the literature regarding transparency and control. Even though control has been a constant theme of privacy dating back to Westin (1966), it can now be extended to the discussion of perceived creepiness, which was found to be distinct from, but related to privacy violations. Transparency is another construct that has been extensively studied (see Chapter 2) and this research provides another domain in which transparency by the firm is important. Additionally, my study provides another construct (perceived creepiness) in which contextual integrity and the violation of context-relative informational norms (Nissenbaum, 2009) can be applied.

My research on perceived creepiness provides an opportunity to add to the literature of online information privacy concerns (Malhotra et al., 2004; Smith et al., 1996; Xu et al., 2012), personalized messages, and the effect of the messages that are perceived to be intrusive and creepy. Chellappa and Sin (2005) stated that there has been limited research on the value of personalized messages given their privacy concerns. This study helps to address that gap.

Consequently, this research is prescient in that “it discerns or anticipates what we need to know and, equally important, of influencing the intellectual framing and dialogue about what we need to know” (Gioia, Corley, & Hamilton, 2012: 13). The application of prescient management theory, in turn, enables scholars to address social changes arising from technological advances, including privacy and artificial intelligence (Gioia et al., 2012).

Implications for Practitioners

The findings from this mixed-method study will be significant to the domains of privacy, marketing, and management of information systems (MIS). If practitioners are aware of the factors that contribute to a personalized message being perceived as creepy, then they can take the necessary steps to help ease or alleviate the behaviors that are causing consumers concern. With these findings, firms will be cognizant of the fact that if they are transparent about their data collection and use practices, and if they provide consumers with control mechanisms, then perceptions of creepiness will be minimized. We also hope that when firms understand the importance of being transparent, they will take the necessary steps to improve how they disclose their data collection and use practices. Providing a privacy notice is only the tip of the iceberg in terms of being transparent. Companies need to take additional measures to protect consumer data, be forthright about the information that they have about a consumer, provide specific information as to how they are collecting, using and sharing this information, provide consumers with a means to correct or modify any information that is inaccurate and allow the consumer to opt-out of receiving personalized messages and or the data collection methods used to capture data without the consumer’s knowledge.

The findings from this research show that, for the most part, consumers enjoy receiving relevant messages and the perks and awards that come along with having their data collected and used, as long as they have some level of control over how that is done, as well as the option to opt-out or stop unwanted messages. The Creepy Quadrant will enable companies to determine in what zone their personalized messages fall and take the necessary steps to move toward the Safe Zone where the firm is transparent, and the consumer has control.

Not only will firms understand how transparency and control impact perceived creepiness of personalized messages, but they will also have an understanding of how the level of trust a consumer has about a company impacts perceived creepiness and how perceived creepiness impacts the companies brand, reputation, customer experience and overall customer satisfaction. Also, companies will be aware of the increased likelihood of messages being perceived as creepy, if they are perceived as being "out of context" as opposed to being "in context." Customer Satisfaction is a critical concept in marketing practice and business management and is often thought to be an outcome of marketing activities, which serves as a link between purchase, consumption and post-purchase feelings (Churchill, 1982). Given the impact of customer satisfaction on repeat sales and brand loyalty (Churchill, 1982), it is incumbent upon firms to understand how personalized messages that they perceive are helping to increase business are actually reducing customer satisfaction and negatively impacting sales and revenue.

Transparency is a major contributor to perceived creepiness, and this is one area in which firms will need to devote more attention. Being transparent and disclosing data collection, use and sharing practices becomes challenging with applications and services accessed on mobile devices with small screens and within the Internet of Things (IoT) where often times the collection of data is incorporated into the infrastructure (Bruening & Culnan, 2015). Bruening and Culnan (2015) question whether the current disclosure and efforts to be transparent are conducive and sustainable within our data-driven society.

Additionally, the findings from this research can be of assistance to data brokers and data aggregators that collect information about consumers, which when combined with data that firms already have about consumers, enable them to create new knowledge or infer information about a consumer that would not have otherwise been available. Data brokers and data aggregators can also take measures to be transparent about their data collection and use practices, just like marketers and other companies. More data brokers can follow the model of Acxiom Corporation that created a website AboutTheData.com (https://aboutthedata.com), which allows consumers to view the data that Acxiom has about the consumer and correct inaccurate information. This is an example of providing consumers with some degree of control over their personal information.

Lastly, this research can add value to the discussion of Big Data ethics, "just because we can, should we?" Research that is supported by empirical data will help practitioners to develop processes to maximize the benefits of using Big Data without tipping the creepy and privacy scales and acting in ways that violate social norms or even perceptions of unethical firm behavior. One must know creepy in order to avoid creepy. Knowing and understanding the factors that lead to perceptions of creepiness will enable companies to create and deliver personalized messages that are perceived to be cool and clever and fall within the Safe zone and not in the Creepy zone.

CHAPTER 6: LIMITATIONS AND FUTURE RESEARCH

Limitations

Despite the best intentions and efforts to generate “perfect” research, no research is without limitations and mine is no exception. It is important to identify those limitations and, to the extent possible, address them or help lay the groundwork for future research. The limitations of my study fall into three broad categories: 1) Sampling universe; 2) Narrow scope of factors examined; and 3) Subjectivity of perceived creepiness, all of which could ultimately impact the generalizability of my research.

Sampling Universe

In Study 1, which was a qualitative inquiry, attempts were made to have a diverse sample. However, the subjects interviewed were within the researcher’s professional and personal network, which were not representative of society in terms of age, educational level and ethnicity. Interviewing more people across a varied demographic may have generated different results in terms of factors that may have been identified that would lead to perceived creepiness. In study two, the majority of the respondents were sourced from Amazon Mechanical Turk; in study three, all of the respondents were recruited from Mechanical Turk. Although it has been stated that their data is diverse and of comparable quality (Buhrmester, Kwang, & Samuel D. Gosling, 2011), it may very well be that the respondents completed the survey for financial gain, although the compensation was approximately $1.50 per completed survey.

The respondents for all three studies were U.S. citizens. Research has shown that different cultures and different parts of the world view privacy and use and or misuse of their personal information differently (Bellman, Johnson, Kobrin, & Lohse, 2004).

Additionally, the laws and regulations in different parts of the country contribute to the sense-making and mental models in which consumers of that country view privacy and unsolicited personalized communication where their personal information and online behaviors are the basis for those communications. Mental models combined with societal norms can affect what is perceived as creepy; therefore, what is perceived as creepy in one part of the world may have a completely different effect in another place.

Narrow Scope of Factors Examined

The factors identified in the first study set the foundation for the next two studies. The findings along with the measurement and testing of the factors surfaced three factors that may lead to perceived creepiness, and I chose to focus on transparency and control, as they were dominant themes. But there may be several other dimensions that may play a prominent role in perceived creepiness similar to that of transparency and control. Had these factors been identified, it could have changed the focus and direction of this research.

Additionally, I did not examine regulations from various levels of government or professional organizations, which could have an effect on companies' disclosure practices and the degree, to which they are transparent about how they collect, use and share data. It may very well be that organizations are taking steps to be transparent as it is a part of their company mission, values or guiding principles, and or governmental enforcement actions may be forcing certain disclosure practices.

Additionally, using the scenario method, I was unable to measure separately the effect of transparency and control in the Surprising and Twilight zones of the Creepy

Quadrant (Figure 1). More research is needed to adequately flush out and test these points along the creepy continuum.

Subjectivity

Perhaps, the greatest limitation of my study is the subjective nature of perceived creepiness. Creepy is a word that is socially constructed and societal norms, and as stated, existing mental models and sense making behaviors play an important role in determining what is indeed creepy. Societal and social norms and what has been accepted as "normal" for a particular culture or point in time may change over time; what is creepy at one point in time may be the norm at another point in time; therefore, determining what is creepy may be somewhat of a moving target. Perceived creepiness is in the eye of the beholder; therefore, it is difficult to determine what "creepy" is with any precision. Although what is perceived to be creepy may change over time, the basic feeling of creepiness, just like other emotions does not go away, nor do the factors or consequences of perceived creepiness dissipate.

All three categories of the limitations have the potential to affect and call into question the generalizability of my study. However, the mixed-method study that was both exploratory and confirmatory across different samples should help to minimize the concerns of generalizability. As the theoretical framework of perceived creepiness is subjected to the application and refinement phases of theory building (Lynham, 2002, Swanson & Chermack, 2013), it is likely that the issue of generalizability and any other shortcomings of my studies will be further addressed and my findings are confirmed to be generalizable and applicable more broadly.

Regardless of the limitations discussed, my study will help in the basic understanding of perceived creepiness of personalized messages and how these perceptions may impact customer satisfaction that ultimately have the potential to impact brand reputation, sales, and revenue. Additionally, the groundwork is laid for future research.

Future Research

Perceived creepiness is subjective in nature and influenced by societal norms. A longitudinal study could be conducted to determine if and how perceptions of creepiness change over time. One could also determine if the factors that I identified are still valid and affecting perceived creepiness or if there are other factors that may surface as more data about individuals becomes available and used in creative ways and ultimately, have a greater impact on perceived creepiness.

This dissertation research was to understand perceived creepiness when personal data is used to deliver personalized messages, but more research is needed on how the collection, use, and sharing of personal information affects ones' life overall. Data and the insights garnered from data analytics continue to permeate every fabric of our life, as every aspect of life is being watched, tracked or monitored in some fashion, moving us toward a "culture of surveillance" (Staples & Field, 2013). Research is warranted on the full impacts of this new norm.

Because advances in technology continue to emerge, such as with Google Glass (Google, n.d.) and the Internet of Things (IoT), understanding the intersection of Big Data, privacy, and innovation is another area worthy of future research. It would be interesting to determine if creative uses of data or data used in unsuspected ways invoke the creep factor or if the benefits and advantages of innovation supersede perceived creepiness. The IoT has been called the next Industrial Revolution and solving for problems that may not actually exist, such as the need for a remote opener for our front door[11].

Even though Big Data, and personal data, in particular, is often used for good reason, there may be cases when the use of data has unintended consequences that are not worth sacrificing privacy and the creepy feeling for the sake of innovation and short term gains. Conventional societal norms and what are the “right” uses of data are becoming murky, so there is a need for Big Data Ethics. Someone has even suggested that Big Data is our generation’s next Civil Rights issue.[12] Big Data as we know it today is a fairly recent phenomenon. As a result, research on the impacts of Big Data on society is in embryonic stages within academic literature, yet there is much to be studied as this is such a dynamic topic. Additionally, revisiting marketing ethics may be warranted as the advent of technology and the plethora of data available about consumers allow marketers to employ various tactics and strategies that were not previously available.

One of the key components of my research was transparency. More research is needed into the transparency of algorithms that are the foundation of customer profiling and segmentation on which personalized communications are often based. As things are constantly changing within the data-driven world in which we live, the landscape is wide open for research covering any aspect of the impacts of data practices and how the uses

[11] Rebecca Herold, Founder, The Privacy Professor, privacyprofessor.org, privacyguidance.com, rebeccaherold@rebeccaherold.com
[12] solveforinteresting.com

of this data impact consumers on a day-to-day basis; in essence the social responsibility of data collection, use and sharing practices.

Appendix A: What is "Creepy"? Towards Understanding That Eerie Feeling When it Seems the Internet "Knows" You (Study 1)

Abstract

With the proliferation of Big Data available, marketers, data brokers, data aggregators, and online advertisers are able to collect personal information and track behavior about consumers and deliver personalized communication that they believe is the right message, to the right person at the right time. Not all consumers view the practice of behavioral or retargeting marketing as clever or coincidental. Rather, they view it as *creepy*. This qualitative methods research moves beyond the theoretical to the experiential and focuses on how people *experience* personalized communication or ads when they perceive it to be *creepy*. What is *creepy*? *Creepy* is a word that has been socially constructed to ascribe meaning to the reality that new knowledge has been created when personal information has been collected and used in a manner that is unknown and unexpected. In order to make sense of *creepy*, the amorphous "they"—which is believed to be in control—is anthropomorphized and social imaginaries as well as other symbols are used to make sense of this experience. At first glance, *creepy* masks as only a privacy issue—albeit, privacy is a component, however, it goes further than that. Amongst other things, our research found that creepy is a continuum and manifests to some degree when the dynamic forces of trust, transparency, and control within a certain context are juxtaposed, which is displayed in what we have called the "Creepy Quadrant."

Keywords: Creepy marketing; social imaginaries; behavioral marketing; data privacy; data privacy.

Introduction

Zappos shoe ads "follow" you on the Internet (Helft & Vega, 2010); Orbitz charges you a different price, depending on the computer you use to access their site (Ong, 2012); Amazon provides you with items that you may be interested in buying or recommends books based on your current book selection; Facebook shows you people that you may know; and you know all of them (Downes, 2012). These are all examples of personal information or behaviors being used to deliver a personalized communication or experience. Through the data collection efforts of Target, they were able to mine the data and glean consumer-buying habits from women and compared it to the buying habits of women who had signed up for Target's baby registries. From this analysis, they were able to predict who is pregnant. In one case, Target sent a young teenager coupons for baby-related items. Her father questioned the store manager as to why his daughter was receiving these coupons only to find out later that his daughter was pregnant; indeed, Target figured out that the teen was pregnant before her father did (Hill, 2012). *Creepy*, clever or coincidental? The above example has been deemed to be "creepy"[13] by many; the fact that Target knew so much about their customers' buying habits and about their pregnancies ahead of time, "*creeped*" people out (Hill, 2012).

In the modern age of "Big Data" (Tene & Polonetsky, 2012) and the data-driven society in which we live, marketers aggregate consumer data and behaviors from several sources in order to gather the necessary information to deliver personalized communication and ads. Marketers want to deliver the right message to the right person at the right time and consumers want to receive relevant ads. However, despite the benefits and ability to deliver relevant communication and ads that Big Data has to offer, the issue of privacy arises and the perils of leveraging Big Data begin to surface. How is it that once the personalized communication or ad is delivered, it crosses the line and becomes *creepy* and even intrusive? Privacy and Big Data as it exists within the public sphere of the Internet (Kelty, 2005) seem to be at opposite ends of the spectrum. Hence, when the two ends of the spectrum converge, the collision of Marketing and Privacy ensues. While some consumers are appreciative of personalized communication and ads,

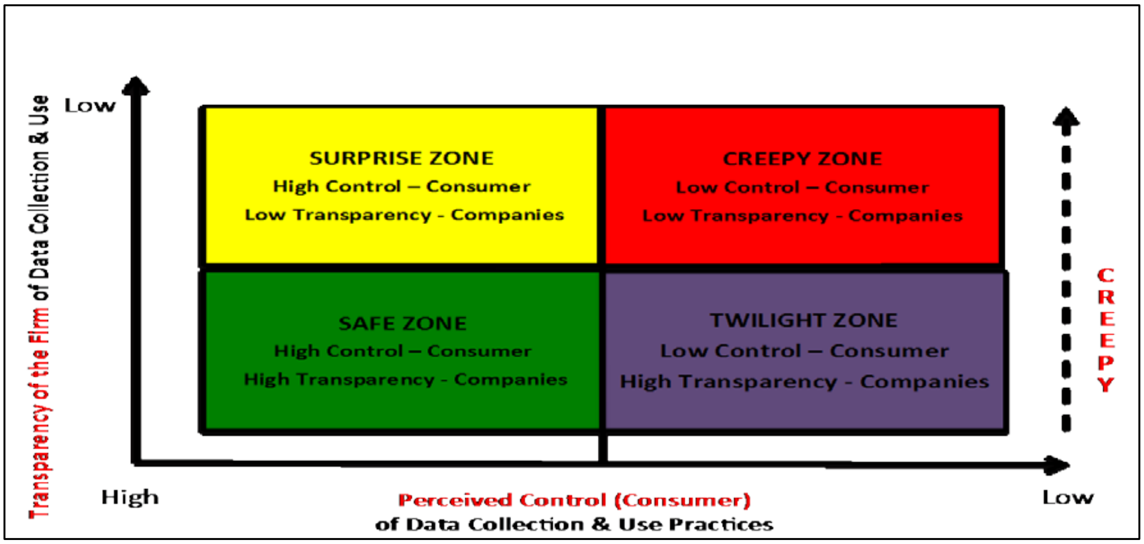
[13] The word "creepy" is in quotations to denote that this word is not a technical or theoretical term, but a euphemism in modern language. Henceforth, the word creepy will not appear in quotations but may be italicized for emphasis.

other consumers and some privacy advocates are describing the things that seem to be relevant as “smart, useful, scary or *creepy*” (Ur et al., 2012: 1). Additionally, a recent study conducted by Harris Interactive found 90% of consumers have concerns regarding the collection and use of their personal data and their privacy online (“U.S. Consumer Findings from Online and Mobile Privacy Perceptions Report,” 2012). Despite the benefits of delivering and receiving personalized communication and ads, consumers are split between those who disapprove of collecting and using personal information in ways that are unexpected with those who believe that an individual should have no expectation of privacy on the Internet. Former Sun Microsystems CEO stated, “You have zero privacy anyway. Get over it” (Sprenger, 1999).

Privacy, from a theoretical perspective, exists in the literature dating back to the seminal works of Warren and Brandeis (Warren & Brandeis, 1890). However, the information is limited as it pertains to how consumers “experience” privacy or react to personalized communication and ads within the realm of behavioral marketing that are unsettling and designated as *creepy*. Thus, the question that our research seeks to inform is: what is *creepy*? and what key factors make a personalized communication or ad *creepy?*

Our research provides insight into the emotional response one experiences on the Internet when a personalized communication—thought to be beneficial—also creates an eerie feeling and pushes the boundaries of omniscience. In order to make sense of the feeling being experienced, we present the notion that from a reality that is socially constructed, social imaginaries are engaged to make sense of those experiences. Further, we introduce the Creepy Quadrant (Figure A1), which displays the interplay of key factors that we found may lead to a personalized communication being perceived as *creepy*.

Figure A1. The Creepy Quadrant


Low
Transparency of the Firm of Data Collection & Use
High
SURPRISE ZONE
High Control – Consumer
Low Transparency - Companies
CREEPY ZONE
Low Control – Consumer
Low Transparency - Companies
SAFE ZONE
High Control – Consumer
High Transparency - Companies
TWILIGHT ZONE
Low Control – Consumer
High Transparency - Companies
CREEPY
Perceived Control (Consumer)
of Data Collection & Use Practices
Low

The findings should be of use to marketers, data brokers, data aggregators and other Internet communication professionals providing personalized communication or ads to help avoid inflicting that *creepy* feeling onto consumers. Utilizing this information could help marketing and other data-driven entities prevent the negative impacts on customer satisfaction, brand, reputation, customer experience, sales and further governmental regulation and sanctions.

Literature Review

Academic research, specifically on *creepy* as a reaction or emotion experienced when receiving a personalized communication or ad, is limited. With the growth of using "Big Data" for data-driven marketing tactics such as behavioral and retargeted marketing, the notion of *creepy* communication is a fairly new concept; thus, research in this area is in the formative stages. To help us better understand what makes a personalized communication or ad *creepy*, we will need to employ an interdisciplinary approach and examine existing literature through the lens of Privacy, Marketing, and Communication. Although the focus of this research is not so much about what privacy is or isn't, reviewing perceived creepiness from that perspective seems most appropriate.

Even though *creepy* does appear in academic literature, the literature is nearly silent in defining *creepy* in the context of marketing messages. What is *creepy*? According to the dictionary, *creepy* is defined as something that is annoying or unpleasant (http://www.merriam-webster.com/dictionary/creepy). Tene and Polonetsky (2013) indicate that there are several things that are perceived as *creepy*, one of which is the unexpected use or personalization of data. Within the marketing domain—particularly from a practitioner perspective—*creepy* is a well-known and commonly used term, most often associated with the reaction to retargeted marketing ads, such as when you view an ad in one online location, and the same or similar ad seems to follow you on another unrelated online location (Stein & Harrell, 2011). According to Downes (2012), the "creepy factor" is a strong emotional response felt when an information service appears to have zeroed in on one's deepest, darkest secret preferences, and Downes (2012) further states that when specific data is used in an unsuspecting way, the initial response is often the *creepy factor*. The *creepy factor* comes into play when something happens that you didn't expect, or hadn't experienced before, and you think: "how did they know that?" Even though a concrete definition of *creepy* is lacking, events such as Target knowing a girl is pregnant before her family (Hill, 2012), enable us to begin formulating a description or definition of what *creepy* is—and more importantly to this research, how it is *experienced*.

Privacy

Privacy is a loaded word. Through the years, it has come to mean different things to different people. Further, there are multiple aspects of privacy. Despite the scholarly research that has taken place within the privacy domain over the last several decades, scholars and practitioners have yet to agree on one definition of privacy, one unified theory of privacy, and even what constitutes an invasion of privacy (Solove, 2006). How privacy is defined, most often depends on your perspective and the lens from which you view privacy. Privacy crosses multiple disciplines, including law, technology, marketing, economics, and information systems; each has a slightly different interpretation of what privacy means. In spite of a lucid meaning of privacy, there are a few theoretical frameworks that can be analyzed which help us understand the context of our research study. As with the theory of privacy, to date, there is also no prevailing theory of *creepy*. Tene and Polonetsky (2013) propose "A Theory of Creepy: Technology, Privacy and Shifting Social Norms" that begins the discussion of a "creepy" theory that takes into consideration new technology and social norms to understand and navigate the "techno-social chaos" (p. 2). Their research embodies the concepts transparency, accessibility to information in a usable format and context which builds upon some of their previous work (Tene & Polonetsky, 2013). In lieu of a unified and comprehensive theory on *creepy*, we will utilize the concepts regarding data privacy as it pertains to the collection and use of data as a starting point to better understand *creepy* relative to personalized communication and ads.

Existing privacy theories and laws have remained somewhat static and have not changed to align with living in the modern world, the virtual world, cyberspace, and the

Internet. Many of the existing privacy theories address privacy in the physical realm, and despite efforts to do so, these frameworks are not easily extended to the virtual world, cyberspace or the Internet. As the landscape of privacy theories are canvassed, Tavani (2007) suggests that they fall into primarily four categories: non-intrusion, seclusion, limitation, and control. Additionally, most privacy theories are normative theories which tend to be rights-based or descriptive, whereby, privacy is understood to mean a collection of personal information that when accessed leads to an encroachment on one's privacy (Tavani, 2007). Other authors have suggested that privacy should be thought of in terms of interest (Clarke, 1999) or property with an economic value (Hunter, 1995; Posner, 1978). Recent literature has reviewed privacy concerns from a more contextual aspect and situation-specific perspective as opposed to general privacy concerns (Xu et al., 2011).

The most prevalent *non-intrusion and seclusion* theories of privacy that provide much of our foundational understanding of privacy is from the law article written by Warren and Brandeis which posits individuals have a right to privacy (Warren & Brandeis, 1890) and freedom from other intrusions to privacy (Bratman, 2001) in essence, the "right to be let alone" (Kramer, 1989). The purpose of this article was to provide direction on how to protect citizens from photojournalists who were using the latest technology of that time—a camera—to take unwanted and unsolicited photographs (Warren & Brandeis, 1890). The "right to be let alone" framework can be extended to Internet activity as it applies to unsolicited or unwelcome intruders (pop-up ads) and support the notion that individuals have a "right to be let alone" (Warren & Brandeis, 1890) on and off the Internet. Although this literature does not directly address the creepiness of personalized communication, it does speak to privacy intrusive behaviors that people experience while on the Internet, some of which have been called *creepy*. This supports our findings that *creepy* and *privacy intrusive* are related, but separate responses, thus a communication may be *creepy* and not *privacy intrusive* and vice versa.

The group of privacy theories regarding *control and limitation* is perhaps the most applicable to the growing discipline of informational privacy and to the findings of our research.

The idea of control, or lack thereof, regarding how personal data is collected and used is another determinant that impacts an individual's attitudes and perspectives regarding information privacy (Culnan, 1993). It's been stated that consumers' privacy concerns in electronic transactions stem from a consumer's loss of control over personal information (Metzger, 2007). Control is a recurring theme associated with information privacy. Many social scientists and privacy theorists have included control as an element in the definition of privacy (Goodwin, 1991). Within the context of marketing and personalized ads, privacy exists when a consumer can limit access and control the flow of information about them; conversely, privacy is invaded when control is lost (Culnan, 1993; Milne & Gordon, 1993; Simitis, 1987).. It is presupposed that consumers want more control over their personal information and having this control will minimize privacy concerns (Phelps et al., 2000). Goodwin suggests that two dimensions of control can define privacy. The first includes control of unwanted solicitation or personal intrusion in the consumer's environment; the second deals with the control of information about the consumer. Both of these factors are applicable to personalized communication or ads received on the Internet and may have an impact on the degree to which a personalized communication or ad is deemed to be *creepy*. Surveys regarding control over how information is collected and used supports this claim (Cebrzynski & Shermach, 1993)

Control theories of privacy have a basic premise that one has privacy if and only if one has control over information about oneself (Beardsley, 1971; Fried, 1990; Miller, 1971; Rachels, 1975; Westin, 1968).. Variations on control theories of privacy include Charles Fried, who takes the position that privacy is more about the control of the information we have about ourselves and less about who knows what about us. He states, in part, that privacy is "the control over the information that we have about ourselves" (Fried, 1990: 54). Arthur Miller states privacy is "the individual's ability to control the circulation of information relating to him" (Miller, 1971: 25). James Rachels refers to privacy as "our ability to control who has access to information about us and our ability to create and maintain different sorts of relationships" (Rachels, 1975: 97). In Privacy and Freedom (Westin, 1968), Westin proposes a theory of privacy, which claims that people protect themselves by limiting access to themselves by other people.

Another key factor in the control theories of privacy is that of choice; that is, the individual has a choice about who can have access to their personal information. Although the control frameworks do not explicitly define what types of personal information one can expect to have control over and how much control one can expect to have, it is suggested that control is limited to "nonpublic information," which includes sensitive and confidential data (Tavani, 2007). When the control theories of privacy are applied to data-driven marketing, one might suggest that the individual does not always have a choice as to what information is gathered and shared when developing a personalized message.

Limitation theories of privacy hold that “one has privacy when access to information about oneself is limited or restricted in certain contexts” (Tavani, 2007: 9). Authors who have written within this realm include Ruth Gavison, who describes privacy as “ a limitation of others’ access to information about individuals” (Gavison, 1980: 428) and W.A. Parent, who defines it as “the condition of not having undocumented personal knowledge about one possessed by others” (Parent, 1983: 269).

A combination of the control and limited access theories of privacy results in the Restricted Access/Limited Control (RALC) theory of Privacy (Moor, 1990, 1997), which has three key elements: non-intrusion, non-interference, and control over/limited access to personal information, with control being a major component of this framework. Control is a mechanism for managing privacy, and the RALC concept allows for a person to have some level of control with respect to choice, consent, and correction. Tavani applies RALC to Data Mining on the Internet (Tavani, 2007), which is the computerized technique that uses algorithms to analyze large amounts of information and allows for the aggregation of data into categories or classifications which enable marketers and other data brokers to provide consumers with personalized communication or ads.

Marketing

From a marketing perspective, scholarly literature on behavioral marketing and its impacts on privacy are expanding as this tactic continues to grow and permeate the marketing landscape. Practitioner literature has acknowledged *creepy* in marketing campaigns, as marketers are becoming keenly aware that what seems like a great idea may be causing consumers angst (Stevens, 2002). Economic literature provides for our review, theoretical frameworks such as Social Contract Theory and Behavioral Economics as another lens in which to review behavioral marketing. The concepts within Social Contract Theory (SCT) support that people are willing to exchange their personal information and negative feelings in exchange for something of value (Friend, 2004). SCT explains the relationship between an individual and a firm when data is exchanged for something of benefit; for example, to access a website or to obtain discounts (Dunfee et al., 1999: 14). The contract is breached when consumers are not aware of how marketers are collecting, using or sharing the consumer's personal information with a third party without permission (Culnan, 1995).

Communication

Communication Privacy Management (CPM) Theory, as defined in the framework developed by Petronio (Petronio & Durham, 2008), supports the idea of managing control over how one’s personal information is used by coordinating what and to whom they will disclose personal information—particularly within interpersonal relationships. CPM is based on a set of rules that enable people to manage boundaries. The rules to disclose are based on five criteria: cultural norms, gender differences, motivations for disclosure, context of the disclosure, and risk-benefit analysis (Cochran, Tatikinda, & Magid, 2007). CPM addresses the tension between disclosure and privacy and examines how and why people decide to reveal or conceal private information across various relational context (Metzger, 2007: 336). This theory posits that once the information is shared, it does not give the recipient of the information full control of the information (Cochran et al., 2007). Further, the individual has an expectation that the information shared will not be shared with others and will remain private.

While CPM theory initially pertained to face-to-face interpersonal communication, the relevance to online communication is clear. Within the context of the Internet, many of the same underlying tenets hold true, especially the notion that one ascertains the risks and benefits before disclosing personal information in an e-commerce relationship. On the Internet, individuals apply the same criteria, such as cultural norms, motivation for disclosure, and the specific situation or context before disclosing personal information (Metzger, 2007). The application of CPM to online consumer interactions provides an understanding as to how people try to protect their privacy online using boundaries to determine ownership of data and who is the actual beneficiary of the data.

Methods

Methodological Approach

This qualitative research used grounded theory methodology as originally developed by Glaser and Strauss (1967), and further refined by (Strauss & Corbin, 2008) and Katherine Charmaz (2003). Although there are differences in the Glaserian, Straussian and Constructionist approach to grounded theory, all support the basic premise of grounded theory—as originally stated by Glaser and Straus—that it is a social science methodology providing a systematic approach to the discovery of theory based on the experience of social actors (Glaser & Strauss, 1967). Grounded theory emphasis is on understanding human behavior through a process of discovery from the data. For our research on how people experience *creepy* in personalized communication and advertisements, the grounded theory method was best suited to gain insight about those experiences. We collected data on the lived experiences of receiving personalized communication and advertisements through semi-structured interviews.

Sample

Our subject universe consisted of individuals who were Internet users and had some measure of computer and/or Internet literacy. We preferred that the interviewees had a higher level of Internet engagement—as opposed to being a casual Internet user—since much of the data used in behavioral and targeting marketing is derived from an individual's online behavior and the digital footprint that they leave behind. Also, more interaction on the Internet allows the respondent to draw upon more lived experiences from online data sharing and behavioral marketing, thus enabling us to gather rich data for our research. However, individuals with limited Internet usage were not excluded since offline and online behavior is often combined when determining whether to deliver a personalized communication or ad. Interviewees ranging in age from 18–64 years old were selected from the personal and professional network of the researcher. Age cohorts were used to categorize the ages because people born within the same time span or generation have common ideas and beliefs in regard to the world around them (Dator, 2009), especially regarding the Internet, social networking, and privacy (Yadav, 2010). The age cohorts used in this study were as follows: Generation Y (Age 18–32), Generation X (Age 33–44), Young Boomer (Age 45–54) and Old Boomer (Age 55–64) (Forrester Research, Inc., 2010).

In an effort to obtain a diverse sample as it pertained to age, gender and race, we were intentional in our selection of interviewees. We observed the interviewees to ascertain gender and race. In an effort to remove any uneasiness in disclosing the interviewee's ages, the question was asked, "What age-cohort do you most identify with?" A document was shown that listed the age cohorts and the respondent selected the appropriate cohort. There were a couple of occasions when the respondent stated their age and the researcher identified the age cohort. There were other occasions when the respondent identified the age cohort based on their age but stated that in their thinking and worldviews, they identified with another age cohort. In the evaluation of the data, those responses were not given any additional analysis to determine if their responses were more aligned with others in their respective age cohort or those of the age cohort to which they identified from the perspective of their ideas and beliefs.

From a gender perspective, 59% of the respondents were females and 41% were males. In terms of race, 41% were Caucasian and 59% were what we would categorize as people of color. Gen X and Gen Y combined represented 50% of the respondents and the remaining 50% were Boomers. Educational level ranged from no college to Doctorate/Professional; 68% held a college degree (Associate, Bachelor or Doctorate).

Data Collection

The twenty-two semi-structured face-to-face interviews took place between June 2013 and October 2013. Interviews were conducted at the preferred location of the interviewee; in some cases this was at their office and in other instances it was in a more relaxed setting such as their home or at the library. Prior to the interview, a form consenting to be audio-recorded and the process for maintaining confidentiality of the interview was reviewed and signed by the participant. A copy was given to each interviewee for future reference. The audio recorded sessions lasted between forty and sixty minutes. A reputable company specializing in transcription services transcribed the audio recordings. The reliability and processes for data security were vetted prior to enlisting this company for the required services. To maintain the confidentiality of the respondents, the researcher secured the audio recordings as well as the transcripts.

Our interview protocol provided direction for the interviews, which consisted of sixteen questions with follow-up probing questions to elicit a narrative on the participant’s experiences, thoughts, and feelings with regard to sharing data and personal information online, privacy and more importantly, the factors that make a personalized communication or advertisement to be perceived as *creepy*. The questions required the interviewees to share their lived experiences (Glaser & Strauss, 1967) about sharing personal information on the Internet and receiving personalized communication or ads that made them feel special, happy, uncomfortable or uneasy. At the end of the interview, the interviewees were asked to define *creepy*; and of all of the examples they had discussed, identify the communication, ad or experience that was most *creepy* and why.

Data Analysis

Consistent with grounded theory methodology (Corbin & Strauss, 2008), data collection and analysis occurred simultaneously and iteratively. This methodology promulgated the process necessary for sound qualitative research. Grounded theory methodology entails gathering the data, writing memos and three stages of coding: 1) open; 2) axial; and 3) selective (Corbin & Strauss, 2008). During the initial coding process, segments of data were assigned labels that best categorized or summarized each excerpt to allow for comparative analysis (Charmaz, 1995). After listening to the audio recordings and reading the transcripts several times, the twenty-two interviews generated 1,356 segments of text that were open coded into 279 total codes, of which 132 were primary codes and 147 were sub-codes. After the open coding, stage two of the process (axial coding) was performed. During this stage, the most significant codes and underlying themes identified in the initial coding process were used to further aggregate and analyze the data. Through subsequent review of the data and thematic analysis, 50 broad categories or high-level themes emerged. Lastly, selective coding was used to relate categories to subcategories (Corbin & Strauss, 1990; Strauss & Corbin, 1998; Strauss, 1987). This level of coding provided a means for the data to be analyzed in the context of the whole, as opposed to segments. The final stage of selective coding resulted in seven themes that formed the nucleus from which our key findings were derived.

The iterative coding process allowed us to fulfill the ultimate purpose of traditional grounded theory methodology in that we were able to use the data to help explain or perhaps, better understand human behavior and experiences of the people being studied (Benoliel, 1996: 413). Further analysis of the data inspired us to reexamine existing literature and compare data based on the emergent themes.

Table A1. Key Codes

SAMPLE OF OPEN CODES	SAMPLE OF AXIAL CODES	SELECTIVE CODES
Relevance	Big Brother	Control
Abusing my consent	Minority Report	Context
Dichotomy of Internet	Online Sharing Violation	Creepy
Monitoring	Privacy	Private
Emotional Reaction to being watched	Targeting	They
Surprised	Disclosure	Transparent
Nervous	Choice	Safeguarding
Intentionality of companies	Crossing the line	
Context Sensitivity	Profiling	
Utility of Ad/Communication	Benefits	
Sovereignty of the Government	Limiting flow of information	
Lacking Control	Unaware	
Obsessing with the Internet	Eerie	

Findings

Details of the five key findings that emerged from the data analysis will be discussed in this section.

Finding 1: The feeling or experience of *creepy* from a personalized communication or ad is widespread.

One of the final questions in the interview asks, “Of all the examples that you shared, which one was the most *creepy*?” The interviewees were probed to explain why the example that they cited was *creepy*. To better understand what was meant by *creepy*, follow-up questions were asked, “what does *creepy* mean to you?” and “what factors made the personalized communication or advertisement *creepy*?” On the surface, these questions seem quite subjective, and perhaps they are. Despite the conundrum of a nebulous definition of *creepy*—the subjectivity and the inherent continuum in which *creepy* exists—the data suggests that the question resonated with the interviewees as all of the respondents provided an example of a *creepy* personalized communication or ad without provocation. None of the respondents asked for clarification as to what was meant by *creepy*, which suggests that there is a common understanding of the term *creepy* and the emotions that it elucidates despite a clear-cut definition. One respondent was keenly aware of the context in which I was referring to *creepy*: “I like science fiction, monster movies, horror. When somebody says *creepy*, that's what I think of. I don't think that's what you mean. I think you meant something that caught me off guard and made me feel uncomfortable, or disturbing” (Education 17).

When the respondents were explaining their experiences with sharing personal information online and personalized communication or ads, the word *creepy* was seldom used. However, upon asking for an example of a *creepy* communication, the interviewee could readily identify what experiences were *creepy*, again, further supporting the normalization of the word *creepy* in our society. This scenario is akin to U.S. Supreme Court Justice Potter Stewarts's description of pornography when he did not have words to describe it but stated "I know it when I see it" (Lattman, 2007; Stewart, 1964). One respondent stated, "but creepy it's overly intrusive, and you know creepy when you feel it" (Education 5).

Synonyms for *creepy* (http://www.merriam-webster.com/thesaurus/creepy) include eerie, haunting, spookish, spooky, uncanny, unearthly, and weird, some of which were used when describing a *creepy* personalized communication or ad.

> "… It's just the spookiness of them posting the ad on something you visited and you didn't purchase, you just visited and you were cruising. It just spooks me out that they know, 'This is you and this is what you were looking at, and we know you were looking at these shoes.' They know the exact shoes that I was looking at and they have a little picture of it" (Marketer 7).

Other words respondents used to describe creepy include: intrusive, disturbing, freaky, irritating, making you feel uncomfortable, overall bad feeling, feeling unsafe, uneasy, and scary. In some instances, the interviewees did not respond with a word to define creepy but encapsulated it with a specific situation or event.

> "I would define creepy as perhaps this coincidence with this … me receiving this United States Postal Service communication when I'm expecting a package. Coincidence or what, I don't know…if I weren't expecting a package" (Professional 15).

> Another respondent defined creepy:

> "I mean if somebody's watching you and stalking you" (Education 5) and "Being watched or being monitored; just all sound like what's going on behind that. That's creepy, that's super creepy or the spam, the random

> spams that are using my ... people on those names to try to get me to believe that it's credible but it's not. That is creepy" (Student 2).

Yet, another respondent associated creepy with being threatened,

> "Yeah, and I think that that whole realm of you know, we start to feel threatened, I think that creepy is you know too much about me, you know" (Marketer10). "Creepy? Like someone sneaking around watching you, just not being legit" (Professional 13).

Similar to the concept of privacy, the meaning of *creepy* is not clear-cut and easily defined, thus, further supporting Potter Stewarts's elusive type of a definition (Lattman, 2007). Although there is a measure of subjectivity when defining *creepy,* most seem to allude to a common theme around control over data collection and use and the surprise factor that their information was collected and used for another purpose than what they intended and done so without their knowledge.

Finding 2: *Creepy* and "Privacy Intrusive" are related, BUT different.

One of the questions specifically asked, "Can you provide an example of when you were on the Internet and you felt that your privacy was invaded or violated?" 12 out of 22 respondents said "no," despite over 80% identifying themselves as "private people."

The respondents seemed to describe being a private person and having privacy as different things as opposed to two sides of the same coin.

> "I'm conscious of what I'm doing in the privacy of my own home, you know, your privacy is like behind closed doors, what you do behind closed doors is your business" (Professional 8).

Being a private person in the context used by the respondents seemed to infer that they did not want to share what they believed to be personal information with people outside of their immediate circle of friends or people with whom they are familiar and had previously provided their personal information.

> “Not personal as in, there's anything wrong with it or, you know, I don't put anything out that I wouldn't want to get to my boss, or my dad, or my sister, or my fiancée, but see, I just don't feel the need to share with people who are beyond my inner circle of friends and family; I felt people don’t need to know where I live or where, I don’t know. I’m just private in that way” (Professional 13).

It would appear as if there was private self for friends and those who are given permission to have access to their private self and a public self, which is open and shared with all.

> “I guess the annoying part of it is I’m a private person. I don’t mind if people know what stuff I’m doing. I’m not doing anything secretive or illegal, but my friends or my colleagues or my students knowing is one thing, but strangers maybe being on the other side of planet knowing everything, I don’t want them to know that. Not that it’s all that hard to figure out, but I guess at my core, I’m a private person” (Education 16).

A few other comments supported the idea of a personal and public self:

> “I don’t want people to be too much into who I am personally. On the Internet, I’m more or so want to put out who I am professionally than personally”; “I don't think that everything needs to be a matter of public record” (Professional 18).

When personal or private information was used in a manner in which they were not familiar or expecting, some respondents did not necessarily feel as though their privacy had been invaded or intruded upon, but described it as *creepy*,

> “It's creepy the amount of information we share online. Because again, we don't know who is on the other end of that Web site” (Professional 8).

Further,

> “I didn't give them that information. I logically can't process how they got that information, so it's *creepy* in the sense that how are people getting this information, what's out there about me that I don't know about, like things that I know are out there about me are: any people search will return

> where I went to school or where I live or where my wedding registry is. That's not *creepy* because I don't like it, but I know why it's out there or that I can find it, but stuff that I didn't know about, about me - that's *creepy*" (Professional 13).

The data supports that *creepy* could be intrusive, but a privacy violation was not always thought to be *creepy*. Creepy and privacy are related but indeed different, despite people responding to perceived creepiness and privacy intrusiveness in a similar manner. Additionally, not knowing who knows what about them also created a creepy feeling.

Finding 3: "THEY" are in control.

Nearly 80% of the interviewees referenced "they" sometime during the interviewee. "They" was the most populous code with 58 excerpts and often occurred more than once during the course of the interview. Seventeen of the twenty-two respondents mentioned "they" during the interview. Ten people said "they" between one and three times, five people stated "they between four and six times and two people talked mentioned "they" between seven and ten times.

Although there was not a direct question which would elicit a response about "they", the interviewees when explaining their experiences with sharing data online would inevitably start their response with "they" or reference "they" as a key actor in their experience. When the respondents spoke of "they," it was more than a casual remark. The interviewees spoke of "they" as if it was understood what was meant or to whom they were referring when they said "they."

To be explicit in the understanding of "they", the interviewer asked a clarifying question, "Who is 'they'"? Although each respondent defined "they" differently, all had created a mental model of whom "they" represented; some of the same characteristics, which were associated with "they", were similar. Initially, "they" seemed somewhat amorphous in nature, as there was not an explicit definition of “they”. It was something that was just out there, without real meaning or substance:

> “It’s the vendors, it's the suppliers, it's the website, it's a generic "they" at this point. We know that there's a lot of data mining going on. It's whoever's placing that cookie on your PC and then tracking you through that cookie. I continue to go back to Amazon, because you see I'm doing that a lot” (Marketer 10); “Whoever the owner ... The popup thing. The ones that track your behaviors, your online behaviors. That's the "they". Whoever is tracking your online behaviors that I am not aware of” (Professional 3).

When the respondents continued to speak of or referred to “they,” the description became anthropomorphic, in that human attributes or characteristics were ascribed to non-human things (Merriam-Webster, 2012). “They” was referenced in a manner in which someone would describe an inanimate object, yet it was anthropomorphized to make it easier to relate and understand. The primary human characteristics possessed by “they” were the ability “to see” and the ability “to know.”

Table A2. Occurrences of “They”

WHO IS "THEY"?	
Amorphous	Anthropomorphic
"They" are People	"They” See
"They" are NOT People	"They" Know
"They" Don’t Exist	"They" Reason
"They" = Government	
"They" = Google	

Despite whether the “they” referenced in the interviews was actually a person or not, “they” was encompassing and the implication was that “they” is “someone” or “something” larger than themselves for which they can’t control. Other characteristics of “they” were more super-human, or god-like in nature, akin to a higher power or something beyond their comprehension or control. It was if “they” was powerful, all knowing and all controlling. Based on the comments from the interviewees, it seems as if in their mind “they” are in control.

> “I don't know what, I don't know what information, but I definitely know they have the information” (Professional 8).

Since the respondents don’t really know who “they” are and they cannot control “they”, their only option is to do nothing and succumb to whatever “they” do. The lack of not knowing who “they” really speak to transparency. “They” are not clearly identified. Respondents were not sure if “they” were online firms, data aggregators, marketers or search engines such as Google. It was also not transparent to the respondent how “they” were collecting, using and sharing their personal information.

Figure A2. “THEY” are in Control Excerpts

"THEY" are in Control
They have to control things but to that extent it's creepy (Student 2).
They have my life out there (Marketer 7)
I mean I know they have my social security number and I know they have my bank account numbers. If somebody wanted to really mess with us (Education 5).
People that run the internet; Whoever runs the internet or marketing through the internet that they could go into every single person’s account and see what websites they’ve been on and then send it on pop-ups that are in those areas (Professional 12).
What do they say in the movie? Who's watching you? Who is watching the watchers? Who is watching you watching? It makes you wonder (Professional 8).

Finding 4: Lack of control as to how personal information is used online led to safeguarding and protecting private or personal information even though there was “nothing to hide”.

Many of the respondents indicated that even though their online behavior may be tracked or monitored, a practice they did not like, they had nothing to hide and were not doing anything wrong. Despite what the respondents said about having nothing to hide, their actions seemed to indicate something different. The respondents went to great lengths to safeguard or protect their identity as well as what they considered to be private or personal information. The respondents were not so much trying to protect their privacy, but control who had access to their personal information and how it would be used. Taking means to safeguard their personal information was not so much of a privacy issue as it was a control issue.

To protect their identity and shield themselves from people outside of their immediate network of friends and family, some respondents indicated that they create multiple email addresses. One email account would be used for family and friends and another email account would be used for the public. The public email address was used when requested by online and offline retailers. Because many indicated that an email address was a form of personal information, the "real" email account was used with people whom the respondents deemed were within their "circle of trust" and felt comfortable sharing personal information which would include family, friends, preferred retailers or retailers in which they signed up for the loyalty program. Another safeguard used was to delete cookies. Although the respondents had nothing to hide, those who deleted cookies did so on a regular basis. In some cases, it was on a daily basis, after each Internet session. One respondent went so far as to use a special script that redirects ads to a bogus server:

> "Somebody built this whole huge script with thousands and thousands of ad sites and tracking sites and they all redirect to your bogus server on your computer, so I no longer get ads. All I get is little X where the ad should've been. I mean I have gone that far to because they just annoy me" (Professional 14).

Other tactics used to safeguard private and personal information was to unsubscribe to unfamiliar email communications, adjust settings on social media and use gift cards for online purchases as opposed to a personal debit or credit card. Most respondents limited the information shared online and only provided what was necessary to complete the transaction. Information sharing on social networking was also limited. There was a common theme that those who need to know, know. The examples above reflect consumers exercising control over the collection, use and sharing of their personal information.

Figure A3. Private and Nothing to Hide Excerpts

SAFEGUARDING NOTHING
I guess or I don't want people looking for me. Not that I'm hiding or have anything to hide from. People that I want to know or people that want to know me or where I am or whatever. They know me or they know who my friends are or how they could find me or how to get to me (Professional 12).
I like to keep things private and my husband is a public servant so he has zero social presence for the media, social media presence (Professional 4).
My close friends know what I do and when I do it. It is not for the whole world to know (Professional 13).
I delete my cookies on a pretty regular basis; I know enough about technology to know that if I clear my cookies, those ads that are looking to find more information can't find anything, because it's gone (Professional 16)
Don't want to be found. This is the reason I have. I feel there is not a reason to have something that points to my … if I want you to know, you will know. Like my friends all know (Professional 6).

Finding 5: Experiencing *creepy* or other negative experiences online does not diminish neither Internet usage nor activities usually performed online.

The benefits of discounts, rewards, relevant ads and being able to see things they enjoy as well as the convenience that using the Internet brings far outweighs any negatives including identity theft, online privacy violations, *creepy* and even the alleged antics of “They” and “Big Brother”. One respondent captures the essence of this finding, which was common amongst other respondents as well with the comment,

> “I know they’re watching … and when I say watching, I mean, they’re studying my behavior and they’re tracking the sites that I visit, which I know they’re doing it and I don’t like it, but it’s my choice to purchase online, so that’s one of the cons, I guess, that I have to live with because it’s my choice, I don’t have to purchase anything, I choose to knowing that they have all this information and they know what I'm doing” (Marketer 7).

Despite respondents being aware to some degree that their online activity may be monitored or used in ways in which they were not expecting, it does not preclude them from using the Internet or sharing data online. The respondents enjoyed receiving extra benefits and rewards from companies with whom they shared information. Also, respondents especially enjoyed the discounts realized in exchange for sharing personal information. Many respondents found the pop-up ads to be annoying and *creepy*, however, this did not deter Internet use. One respondent indicated they like seeing the shoes on the side because they like the shoes and seeing something that they like made them happy. Another respondent had a similar comment in that he enjoyed seeing from time to time an item that he searched for online because he liked the item. Convenience of the Internet along with having the world a click away was another reason why respondents would not stop using the Internet. As evidenced in the data by the amount of time spent on the Internet, it is clear that using the Internet is intertwined into almost every aspect of life including shopping, banking, research, and even socially. The cons of sharing information online are far outweighed by the pros; thus not using the Internet is not an option. Hence, the privacy paradox (Awad & Krishnan, 2006).

Figure A4. Creepy Does Not Diminish Internet Usage Excerpts

"CREEPY" DOES NOT DIMINISH INTERNET USAGE	
I was expecting this because my girlfriend is like, "you should sign up for the birthday club." They used to give you free meals. Now you only get something off. It is just like, "you get a free meal for your birthday", and so I did do that, but I did that knowing that they are going to sell me something (Professional 3).	*I may have went online and got it online because it was a better deal. I have done that. If it's a better deal online, yeah, I definitely shop online (Professional 9)*
Some sites, you know, I want to be marketed from, so there are some vendors, some online sites that I'm willing to provide that information to, because I want marketing from them. And I want offers from them. So other than that, like I get offers from Bob Evans or Ruby Tuesday or restaurants right, whatever it is, and they're pretty valuable. So I'll do that, Amazon or I have bought at Astors, a place called CR Trading Post, which is a huge, they've got a lot of outdoor equipment, usually discounted. So I'll sign up for their e-mails (Marketer 10).	*When I am purchasing something online, I feel it's appropriate to share the information I need to get the product or service. I don't have a problem doing that. It's usually fine. I don't think I've had any negative (Professional 15).*
I just bought a pair of shoes literally last week. I went to Kohl's and I saw a really nice pair of shoes that I liked. I tried them on they were great and, as I'm at Kohl's, I thought they were expensive. As I'm sitting at Kohl's I do a quick search for the pair of shoes and I found the pair of shoes $20 cheaper online. Same size, okay, purchased them right there. Two days later they're at my house okay. It's such a cool thing because you can really find things much cheaper. You know I'm at Kohl's and I find a pair of shoes and sorry Kohl's I'm not spending my $70 with you when I can get it for $50 (Education 5).	

Discussion

The purpose of our research study was to develop a definition of *creepy* as well as identify the factors that lead people to experience and perceive a personalized communication or ad as *creepy*.

In the modern world, modes of interaction, communication and the way in which we live and function is changing due in large part to the rapid advancement of technology and innovation. Data is the driving force in most of what we do on a daily basis.

According to Kuneva, “personal data is the new oil of the Internet and the new currency of the digital world” (World Economic Forum, 2011). In fact, approximately 98% of all stored information is digital (Cukier & Mayer-Schoenberger, 2013). With the increase of big data and expanded use of the Internet, personal information or data is being collected and used in ways that exceed our comprehension. We now have the ability to quantify aspects of the world and transform information into quantifiable data, a process known as datification. Through this process almost everything can be “datified”: words, location, tweets, likes and even friendships (Cukier & Mayer-Schoenberger, 2013).

Our findings support that the perception of *creepy* personalized communication and ads is widespread. With much of personal information and behaviors being “datafied”, it is apparent that when this data is aggregated and presented in unexpected ways, the notion of *creepy* emerges. As we continue with the datafication process and new knowledge is being created in unsuspecting ways, personalized communication and ads that are *creepy* will not go away, but will become more pervasive.

Similar to the concept of privacy that has changed over time and continues to be redefined as society and social norms change, so is the meaning and perception of *creepy* which is dynamic and always in motion. Perception is reality, and the definition of *creepy* will depend on how the meaning of *creepy* is socially constructed and interpreted at a given point in time. Personalized communication and ads that are perceived as *creepy* now may be the norm at another point in time. Over time, what was once *creepy* is no longer *creepy* because consumers adjust to a new normal, and society continues to reshape and readjust to social norms.

Defining privacy requires a familiarity with its ordinary usage, but this is not enough since our common ways of talking and using language are riddled with inconsistencies, ambiguities, and paradoxes. What we need is a definition which is consistent with ordinary language, so that when one speaks of privacy, there is no ambiguity in the meaning that would prevent us from talking consistently, clearly, and precisely about the family of concepts to which privacy belongs (Parent, 1983: 269).

This thought from Parent can also be said about the word *creepy* and what it means when one says that the personalized communication or ad is "creepy."

Most often privacy and *creepy* are linked together; our research suggest otherwise, and although related, the two concepts are different. At the onset of this epistemological study, privacy seemed to be at the core and the perception of *creepy* was deemed to be a privacy issue. As such, our initial literature review was focused on privacy, specifically data privacy and the impact on one's privacy when their personal information is collected and used for marketing purposes.

Our findings suggest that while privacy may be component or play a role, the perception of *creepy* goes beyond privacy. Although *creepy* may seem like an intrusion of one's privacy, not all intrusions on privacy are *creepy* and not all *creepy* communication is privacy intrusive. To explain those personalized communication or ads that are equally *creepy* and privacy intrusive, our research promulgated us to create a new word, "creepacy." *Creepy* is not so much about what privacy is or is not, as much as it is about how people make sense and ascribe meaning to an experience where they are the center of attention, in that their personal information is collected to create new information and knowledge, but they have limited control over how this personal information will be used.

It is through the lens of structuration and social construction where social norms emerge and help to inform how we process the environment and make sense of the world in which we live. That which we socially construct is alive and real. Our research furthers this discussion in understanding *creepy* and making sense of the modern world.

In order to make sense of *creepy,* social imaginaries are elucidated. As the moral order of society has evolved over time from that of a normative moral society to an economy existing within a civil society (Taylor, 2002), social imaginaries help to explain the modern world in which we exist. Social imaginaries enable us to make sense of the practices of society. According to Taylor, social imaginaries embody the ways in which ordinary people imagine their social existence and surroundings, which are seen in images, stories and legends that people pass along (Taylor, 2002). The interviewees for this research are prime examples of sharing their lived experiences relative to sharing personal information online and the resultant *creepy* feelings. Unlike some social theories, the social imaginary is shared by large groups of people or even the society. During the interviews, the respondents did not always say *creepy* when sharing their experiences; however, when they were asked about *creepy,* they had an example. Taylor states, “the social imaginary is that common understanding that makes possible common practices and a widely shared sense of legitimacy” (Taylor, 2002). Engaging social imaginaries, fictional characters, myths and symbols to help make sense of something that cannot be readily explained are not new.

Looking at Orwell's *1984* (Orwell, 1986), "Big Brother" was a term or fictional construct to explain the notion of being tracked and monitored. The term "Big Brother" has maintained its buoyancy throughout the years. What was fictional has become real in the sense that when the term "Big Brother" is mentioned, there is a common understanding among many Americans about what the term means. Big Brother, as well as Big Brotherism, is listed in the Merriam–Webster dictionary (2015) signifying, "authoritarian attempts at complete control (as of a person or a nation)." In fact, the term Big Brother was mentioned multiple times when interviewees in the study were discussing their experiences with sharing personal information online.

> "It just spooks you out because they're tracking your behavior. It's like Big Brother, it's like somebody watch … and I know no one's watching, it's just that I get that. It's just someone watching what you're doing, and they can probably pull you up and they know your likes. It's like getting into your personal life, the style you like. It's like getting to know you without you letting them in to get to know you; that's my opinion" (Marketer 7).

While another respondent did not expressly say Big Brother, the implications are the same:

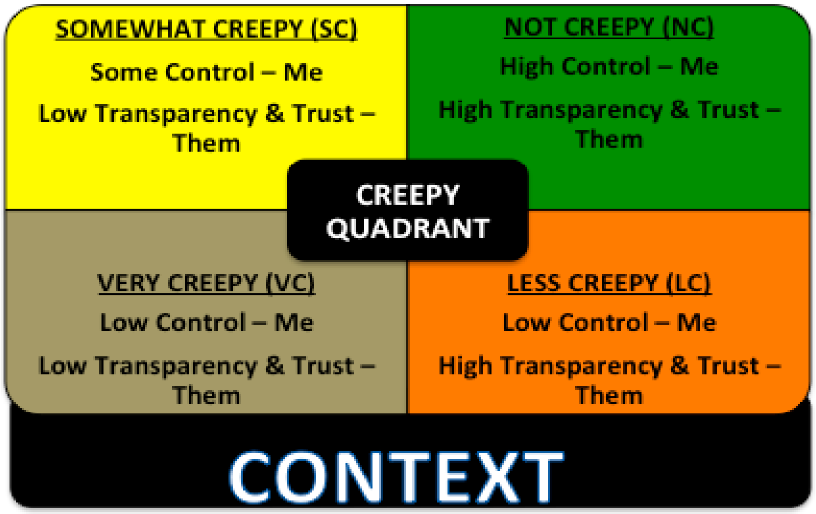
> "I don't want to say it that way. I think the government. They even tell you that certain things they're trying to put in place as laws to really watch, but I think the government does watch every little thing. Everybody says they do, especially online, because of terrorism or just because they're nosey, one of the two" (Professional 19).

The process of constructing reality is most often brought about through social interaction, be it real or symbolic. "The social construction of reality is a dialectical process in which human beings act both as the creators and as products of their social world (Adoni & Mane, 1984). Within this dialectical process, there are three types of reality: 1) objective social reality, which exists outside of the individual and presented as facts; 2) symbolic social reality, which refers to any form of symbolic expression of objective reality such as literature, media or art; and 3) subjective social realities, where both the objective and symbolic realities are inputs for the construction of the individual’s own subjective reality (Adoni & Mane, 1984). It is in this realm of reality that the notion of *creepy* exists.

Another component of *creepy* was the presence of “they”. Since the respondents felt as if they had little control over the collection and use of their personal information, somebody or something had to be in control; research findings support that “they” are in control. Again, in order to make sense of the modern world and the amorphous “they”, the respondents anthropomorphized “they” as another way of making sense out of something that is not readily explainable. Without much thought, people tend to anthropomorphize for several reasons, one of which is “effectance” motivation that is to use familiar concepts to understand environments, including non-human agents (Waytz & Morewedge, 2010). The notion of anthropomorphizing non-human agents enables one to make sense of, predict and even have some level of control in an uncertain environment (Waytz & Morewedge, 2010).. The term anthropomorphism: “anthropos”—from Greek: man, human being, and “morphe”—from Greek: shape form, refers to “human likeness” rather than to “humanness” (Zawieska, Duffy, & Sprońska, 2012: 2). Another aspect of anthropomorphism is to attribute human-like characteristics to non-human agents. According to the interviewees, “they” could see, think and know. Culture and societal norms also contribute to the characteristics one associates with a non-human entity. In the Western culture, seeing or vision is an amalgam of knowledge and power (Cohen, 2008). This is evident in the references to Big Brother from our respondents who implied that Big Brother was watching, knew things about them and was in control.

Key factors that we found that contribute to a personalized communication or ad being *creepy* include context, control, transparency, and trust. All of these factors have been extensively studied within the privacy domain, and arguments exist on both sides the degree to which privacy is impacted by these various factors (Pavlou, 2011; Smith, Dinev, & Xu, 2011). The emphasis of our research is not on whether these factors impact privacy but the extent that they have in the perception of personalized communication or ad as creepy. The mere presence or absence of these factors does not necessarily make a personalized communications or ad to be perceived as creepy. The data corroborates that the interplay, conjoining or juxtaposition of these factors is a greater determinant of whether a personalized communication or ad is perceived as *creepy*. The "Creepy Quadrant" was developed to better visualize the interconnectivity of two important factors that make a personalized communication or ad *creepy*—transparency and control.

Figure A5. The Creepy Quadrant 1.0



The Creepy Quadrant (CQ) has context as the foundation in which the *creepy* continuum, that includes control, transparency and trust exist. Context is key

(Nissenbaum, 2004). *Creepy* is a continuum as are the other factors, so it is the degree that these factors are present which will suggest whether the personalized ad or communication is *perceived* as *creepy*.

As it pertains to privacy, trust is critical. We purport that trust plays as vital a role with perceived creepiness. If consumers trust a company to safeguard their data and act in their best interest, they are more willing to share personal information. A survey conducted by Harris Interactive on behalf of TRUSTe concluded that 95% of adults expect companies to protect their privacy online (TRUSTe Privacy Index, 2012).

> That's the thing because it's Facebook. If it's like some other random websites that I didn't find useful, then it would be different, and I can stop going to, but it's Facebook. I felt like I want to believe that the Facebook people are doing it in my best interest, and they're trying to accommodate me because they think this is what I like instead of going to a random website that has pop-ups and I'm like I don't need this” (Student 2).

Some of the respondents indicated that they only go to sites that are well known and for which they had previously visited, and the outcome was positive. If they were not familiar with the company, they became more leery of what may happen on that site. Additionally, if consumers do not trust the website, it is highly likely that they will not shop on that site.

> “I try not to go on just random. If it’s not Hollister or Sephora or Nordstrom or like a sure store that if it’s someone I don’t know, then I’m not as likely to offer to put that information on the computer and send it to someone” (Professional 12).

According to Miyazaki, consumers often lose trust in companies that do not disclose their use of cookies to gather information about a consumer’s behavior on their website (Miyazaki, 2008). This can occur when transparency is low, and the amount of control over their personal data is limited. When consumers are not fully aware of what is going on with the personal information that they share combined with the notion that they have little control over their data, the *perception* of *creepy* intensifies. In these instances, the personalized communication or ad ranges from “very creepy (VC)” to “somewhat *creepy* (SC)”. On the other end, there is high trust for the company and their website, and the perception of *creepy* ranges from “less creepy (LC)” to “not creepy (NC)” depending on the level of transparency and control.

Transparency is another factor taken into consideration when individuals perceive that their privacy has been intruded upon or violated. To the extent that an individual is aware of the information that is collected and used about them, the less they feel that their privacy has been violated. Surveys conducted in the past clearly indicate the many consumers are concerned about what companies know about them and moreover, how that information is collected and used (“Equifax Consumers Privacy Survey,” 1994, 1995, 1996; Katz & Tassone, 1990). The degree of transparency is another determining factor of perceived creepiness.

Control or the lack of control over how one’s personal information is collected and used was another predominant theme in our findings and is also a vital component of The Creepy Quadrant. Our findings suggest that the level of control an individual had over what personal information was collected and used, who was using it, and how it would be used were primary factors as to whether a communication that utilized the personal information was perceived as *creepy*. Extensive research on privacy as control date back to (Westin, 1968) and Altman’s (Altman, 1975) theories of privacy; since that time other privacy scholars have researched control and its relationship to privacy (Culnan, 1993; Kelvin, 1973; Margulis, 1977; Smith et al., 1996). Control over the secondary use of information as discussed within the privacy domain can also help to explain *creepy* personalized communication or ads. According to Culnan, secondary use of information is the use of information for a purpose other than what it was provided for in the initial transaction (Culnan, 1993). The practice of “the secondary use of information,” now referred to as repurposing is widespread. With each transaction, companies collect data about their customers, which is available for them to use in another context. Although this is legal, it can be experienced as a violation of privacy (Culnan, 1993) and to some even *creepy* if the consumer is not aware of what is going on with their data. With the advancement of technology and other privacy enhancing technologies, privacy concerns tend to escalate (Culnan, 1993). However, our research suggests that despite *creepy* and other negative experiences, neither Internet usage nor the activities performed online are not diminished.

Limitations

No research is without flaws or limitations, and this research is no exception. While attempts were made to interview a wide spectrum of people, the interviewees were within the principle researcher’s network that may have prevented the interviewees from being fully forthright about the personal information that they share and their online behavior. Additionally, being audio recorded may have also prevented the interviewees from full disclosure. In an ironic way, the essence of our findings, which were centered on the notion of people being ambivalent about being recorded or “watched”, may have limited the extent of their responses. This was evidenced when the recording stopped; the interviewees would elaborate on something that they mentioned during the interview or provide additional examples of personalized communication or ads that they felt were disconcerting. The information provided during those conversations was captured in handwritten notes. Although it was communicated that the information shared would be kept confidential, several people asked about the nature of the research study and how their information was going to be used.

In June 2013, Edward Snowden, former National Security Agency Systems Analyst exposed classified and confidential documents and alleged that the United States Government had been involved with collecting phone records, buddy lists, and mining data on U.S. citizens which piqued peoples' interest about privacy (Estes, 2013). Several respondents referenced Snowden in their responses. The Snowden issue also raised the awareness and concern as to how personal information and data created offline and online is aggregated and used in ways to create new knowledge about them that they were not expecting. If this issue were not in the news and top of mind, the responses alluding to "Big Brother" may not have been as prevalent or perhaps even non-existent.

The principle researcher has worked in Direct Marketing within a financial institution as well as in the areas of information privacy and data governance and has an affiliation with and certification from the leading association of privacy professionals across the world. The principal researchers' relationship to privacy, along with the experiences, opinions and thoughts may have some bearing on the interpretation of the data from the interviews. To offset any bias that may impact the interpretation of the data, advisors provided insight to ensure that the integrity of data was maintained and reviewed with objectivity.

Implications for Practice and Future Research

Implication

The findings in this research can be beneficial to the actors within the data ecosystem who are primarily responsible for data collection and use: companies, marketers, and data brokers/aggregators.

Companies. Our findings suggest that individuals are concerned about how their personal information, however they define it, is collected and used by companies often times without their knowledge or consent. The findings further suggest that consumers feel as if they have limited, if any, control over the process of data collection and use, as information is gathered from disparate sources. Further, there is a feeling that companies are not doing enough to protect personal information when it is shared online. As consumers become increasingly leery of organizations and even the government regarding their data, the manner in which they share personal information on and offline will be altered.

To ease consumer concerns regarding *creepy* communication, companies need to be more transparent about their data collection and data use practices. Providing this information in a privacy notice is just the beginning of the level of transparency needed. Companies need to be forthright about what data they have about a consumer and specifically what they are doing with this information. Another level of transparency would be to disclose how data collection and use are executed upon. For example in the case of Target, they continued their marketing practices; however, it was more subtle; thus, they were not as transparent on how they were executing on the data they had collected (Karvounis, 2012)(Karvounis, 2012). The Creepy Quadrant (Figure A5) shows that if transparency and trust is high, the personalized communication will be less *creepy*. A recent survey indicated that 80% of consumers are willing to share personal information if they are asked up front, and it is clear how the information will be used (PwC, 2013). Some respondents felt as though companies were abusing and or misusing their personal information, thus providing a less than positive customer experience. The data imply that if the individual does not have a comfort level with the company or website, they will forgo any benefit that may be derived from that site to go to a site that they feel is more reliable and acts with integrity in regard to their data usage practices.

Many companies indicate that the customer is "number one" and at the center or core of their business, yet they violate the consumers' trust and act in a manner that disregards consumer sentiment around data privacy. Lack of sensitivity to consumer concerns can lead to *creepy* ads because transparency and trust are low and the consumer has little to no control over their personal information. Understanding consumer feelings around data collection and data use provides an opportunity for companies to be proactive in safeguarding their customers' personal information whereby increasing the trust relationship between consumers and companies, which in the long run may positively impact company sales and revenue growth.

Marketers. Marketers and those delivering personalized communications and online ads should have an appreciation for data from this research as it provides an opportunity to understand customer feelings and expectations around online data sharing and information privacy. Our findings suggest that customers enjoy the convenience of the Internet and enjoy relevant ads to the extent that they have some level of control over how their personal information is collected and knowledgeable about how the personal information that they share with a company is being used. This would require marketers to be more transparent about their online behavioral marketing practices.

With the proliferation of the use of "Big Data", marketers should want to position themselves in a manner in which they utilize the insights that "Big Data" has to offer without personalizing a communication or ad to the degree that it crosses the line and invokes the "creep factor". As marketers utilize all that "Big Data" has to offer, understanding the interplay of control, transparency, trust and context will enable them to deliver ads that are "clever" and not "creepy."

Marketers should take a proactive role in being transparent with consumers regarding the collection, use of consumer data and the information that they have about individuals. Using the Creepy Quadrant (Figure A5) as a barometer, marketers can identify where they fall within the Quadrant at the company level or preferably at the campaign level. Understanding into what quadrant they fall may help to predict response rate. If a consumer's initial response to an ad that marketers think is cool and clever is *creepy*, the consumer may be less likely to respond to the call to action.

Data brokers/aggregators. Data brokers and aggregators would also benefit from the knowledge that consumers are becoming wary about the collection and use of their personal data. While the data brokers and aggregators are not directly responsible for delivering the personalized communication or ads that are *creepy*, they are responsible for collecting information and aggregating it in a manner that creates new information about a consumer that they did not initially provide to the beneficiary of the data. The collection of a myriad of data elements from a variety of sources provides companies and marketers with information that they would not have been privy to otherwise.

Consumers, governmental authorities nationally and across the globe are becoming increasingly dismayed with the practices of data brokers and data aggregators. Even though they have the right to collect the information that they do, the question becomes is it *right* to sell this information that may be used in ways that disregard consumer concerns about information privacy and *creepy* communication. Data brokers and data aggregators can take measures to be more transparent and provide consumers some level of control over the information that they have. Acxiom Corporation, a data broker who maintains vast amounts of data on an individual, launched a website in 2013, AboutTheData.com, that allows consumers to access the website, view their personal information and correct inaccurate entries. This is an attempt at being transparent to the consumer about what data is available about them and providing them with some measure of control over their personal information. Acxiom was praised by the Federal Trade Commission (FTC) and privacy advocates at their attempt to be more transparent in their data collection and use practices (Singer, 2013).

Overall, findings from this research study begin to provide a lens from the individual’s perspective regarding *creepy* personalized communication or ads, how its meaning is constructed and key factors that contribute to a *creepy* communication.

Future Research

While this research was centered heavily on online data sharing and use, further research can be done to determine how the findings in this study withstand face-to-face data sharing and use. For example, if you go to a teller at your bank and without provocation or any related activity, the teller asks how you enjoyed a restaurant because the name of the restaurant displayed in the list of transactions on your credit card, which can be seen by the teller when you come in the branch to make a deposit. It would be worth researching to see how the "creep factor" would be impacted in this type of scenario and offline in general. Would this exchange be perceived as creepy or a friendly gesture by the teller to engage in conversation? While there still exists an online component since the data is stored online in a database, the manifestation of this data occurs in person.

Another key area of related research is online privacy in general and privacy in cyberspace. Since the traditional rules, rights, expectations and norms of privacy continue to evolve, researching the extent social norms have impacted or shaped our views in this discussion may be of interest. As advances in technology continue, such as with Google Glass (Google, n.d.) and the Internet of Things (Chui, Loffler, & Roberts, 2010), many of which entail the use of personal data from various sources as well as derived data from individual behavior and the advent of sophisticated monitoring and tracking devices in our "culture of surveillance" (Staples & Field, 2013), understanding the intersection of privacy and innovation and its impacts on perceived creepiness is also worthy of further research.

If indeed, societal norms and social imaginaries do inform the meaning we ascribe to various terms such as *creepy* as our research asserts, perhaps a longitudinal study could be done to validate if in fact, the meaning or how we make sense of our experience relative to *creepy* personalized communication or ads, privacy, Big Brother and "they" change over time.

As privacy affects nearly every fiber of our life and to the degree we understand how people in general and within different demographics experience privacy, more inroads can be made to develop products, services, and practices that do not invoke the "creep factor".

Lastly, the findings of this research will help to prime a quantitative study that will test the factors that may lead to perceived creepiness. Further exploration of the "Creepy Quadrant" should take place to ascertain to what degree the relationship that appears to exist in the qualitative data between transparency, trust, control and context is statistically significant.

Conclusion

As advances in technology continue, it will be incumbent for actors within the personal data economy and ecosystem to eschew the collision of Marketing and Privacy and coexist in a manner whereby insights of Big Data are used to deliver personalized communication and ads in a way that is relevant while not crossing the line and becoming *creepy*, too invasive and also ensuring that customers feel that their privacy is respected and not violated (Spector, 2012). Our discussion began with "what is *creepy*?" and it concludes with the same question, "what is *creepy*?" The old adage that some things are "better felt than telt" helps us better understand *creepy* and social imaginaries help us to put into context something that is quite elusive and difficult to explain. Bottom line, there is not a "dictionary" definition that will define *creepy* in the context to which we are referring, but the construction of social imaginaries gets us closer to something that we can all agree upon as the norm at a particular time.

Appendix B: Demystifying Creepy Marketing Communications (Study 2)

Abstract

Marketers, data brokers, and online companies collect personal information from consumers often times without their knowledge and for ways in which they did not intend by tracking and monitoring online activities. Online companies use this information to provide targeted communications, advertisements and tailored customer experiences. While consumers do sometimes realize the benefits of these communications, there are some instances where consumers feel that their privacy has been violated, and other times feel as though the messages are "creepy." Privacy violations and perceived creepiness are related but different. We define "creepy" as an emotional reaction to an experience, interaction, technology or unsolicited communication where personal information has been collected with your knowledge or unknowingly and used in an unexpected or surprising manner invoking negative feelings. Utilizing a quantitative approach, we measured several key factors that may have an impact on whether a personalized advertisement is perceived to be creepy. Our results showed that perceived creepiness is impacted by online information privacy concerns, transparency and control. While the insights obtained can help to further the discussion around Big Data and its impacts on privacy, more importantly, practitioners can use this information to create communications that do not cross the line from being helpful, cool and smart to creepy. Further, companies cannot just rely on the fact that they have a trusting relationship with the consumer as we found that trust does not have a mediating effect on perceived creepiness. Companies that can address this issue may benefit from consumer privacy being a differentiator in the marketplace; however, companies that do not get this right stand the risk of damaging their brand reputation, reducing customer satisfaction, customer loyalty and ultimately sales and revenues being negatively impacted.

Keywords: Creepy marketing communications; personalized online advertisements, transparency, control, online privacy concerns, trust, behavioral marketing; data privacy; Big Data ethics.

Introduction

Everything that we see is a shadow cast by that which we do not see.
(Dr. Martin Luther King, Jr.)

Everyday consumers leave behind tremendous amounts of personal information from their routine daily activities, unknowingly creating a digital shadow. From the moment one wakes up in the morning until they retire to sleep at night, almost every detail of life is being captured through phone activity, text messages that are sent, purchases that are made, pictures that are posted, interactions on social media and one's location at any moment in time. "People always leave traces. No person is without a shadow" (Mankell, 2011). All of the pieces of information left behind help create an individual's digital footprint. Purveyors of consumer data, especially marketers, find this information quite valuable as it allows them to make inferences about one's behavior along with their likes and dislikes, in order to provide more targeted personalized communications and advertisements in what they believe is the right ad to the right person at the right time (Double Click Website, 2011). Marketers believe personalized communications create a better customer experience, build a better relationship with the customer, increase response rates to ads and ultimately drive performance with higher profits (Arora et al., 2008).

The problem is that not all consumers view these personalized messages or behavioral-based advertising as relevant, useful, clever or coincidental, but as "creepy"[14] (Ur et al., 2012). According to Arora et al. (2008), another concern of personalized messages is centered on privacy violations. A recent study conducted by GfK in March 2014 (GfK, 2014) indicated that nearly 88% of U.S. Internet users are concerned over the collection, use and sharing of their personal information while online and the additional information that is derived or inferred about them from predictive data analytics.

At first glance, personalized messages may be viewed as *only* violations of privacy. However, there are personalized messages that are perceived to be creepy and

[14] The word "creepy is in quotations to denote that this word is not a technical or theoretical term, but a euphemism in modern language. Henceforth, the word creepy will not appear in quotations but may be italicized in some instances for emphasis

those that are violations of privacy; though they may be related, they are indeed *different*. Not all personalized messages violate our privacy and not all personalized messages are perceived to be creepy, and yet, there is a subset that is perceived to be both creepy and a violation of privacy, for which we coined the term "creepacy."

The purpose of this research is to determine if the factors that were identified in a prior qualitative study—control and transparency, along with a few other factors; online information privacy concerns, perceived anonymity and perceived surveillance—do contribute to a personalized advertisement being perceived as creepy. Using quantitative methodology, we conducted an online survey to address the following research questions: 1) To what extent do online information privacy concerns (collection, use, control and general), perceived surveillance, perceived anonymity and transparency affect an unsolicited personalized marketing communication to be perceived as creepy, and 2) To what extent does consumer–firm trust mediate these factors on perceived creepiness?

To better understand perceived creepiness, we rely on theories within the privacy domain due to the relatedness of perceived creepiness and privacy, along with marketing, trust and communication disciplines to further guide our theoretical direction.

Although there has been prior research regarding marketing communications that may violate privacy, research on personalized marketing communications that are perceived to be creepy has not been widely studied; thus, our research study helps to further the conversation in extant literature to understand perceived creepiness and unveil what is really behind those unsettling feelings. While the insights obtained from this research can advance academic literature, it is most beneficial to the practitioner community; so that they can create personalized messages that are useful and not invoke feelings of disconcertment which can impact consumer–firm trust, brand reputation and ultimately, sales and revenues.

In the remainder of this paper, we will discuss the theoretical framework underpinning our research, provide an analysis of the data, discuss key findings and briefly state the limitations and implications of our research study from an academic and practitioner perspective.

Theoretical Framework

Our interest in understanding *creepy* has increased over the past several years as this word is often used in a marketing context to describe various communications that use consumer data in a surprising and unexpected way and that seem to know us and reveal to us that new knowledge about us has been created. Additionally, the term *creepy* has been associated with technology designed to seemingly know us, almost better than we know ourselves (Keenan, 2014) and leaving us with an unsettling feeling. Despite our interest in this phenomenon, perceived creepiness has not been extensively studied in academic literature in the context of personalized messages, online marketing or consumer privacy. A quick search on Google of "creepy marketing" reveals several entries of articles advising marketers to not be creepy in their personalized marketing tactics. One such article is, "Is Personalization Creepy?"[15] where several marketers provide a discourse on this topic. Other articles include, "Forget Evil, Don't Be Creepy" (Dooley, 2012) and "Be Relevant, Not Creepy" (Spector, 2012). While marketers are admonished to not be creepy, within the literature, there is neither a unified definition of creepy nor the factors that lead a personalized communication to be perceived as creepy.

[15] http://blog.hubspot.com/marketing/marketing-personalization-creepy

Several authors have ascribed meaning to *creepy*. Tene and Polonetsky (2013) purport that behaviors, which invoke perceived creepiness, are not necessarily illegal or circumvent privacy regulations, but tend to grate against social norms and infer that it is invoked when data is used in expected ways. According to Keenan (2014), “creepiness is an elusive concept that tap into our primal fears and assumptions about the way things are and should be” (p. 16). Downes (2012) suggest that the “creepy factor” comes into play when something happens unexpectedly to you or that you had not experienced, and you wonder, “How did they know that?” Perceived creepiness challenges our assumptions and has us wondering how marketers got our name (Culnan, 1993). These references to *creepy* acknowledge that *creepy* exists and when it is apparent, but still do not fully define exactly what is meant by the word *creepy* in the context with which we are referring. Thus, we have established a definition of *creepy*, in the context of marketing communications, as “an emotional reaction to an experience, interaction, technology or unsolicited communication where personal information has been collected with your knowledge or unknowingly and used in an unexpected or surprising manner invoking negative feelings.

Although we specifically reference marketing, this definition can be expanded to include other encounters, interactions or technology that causes one to feel eerie and unsettled.

Based in part on the findings from our prior qualitative study, we were able to identify several key factors that contribute to a personalized communication to be perceived as *creepy*: Online Information Privacy Concerns, Transparency, Control, Perceived Surveillance and Perceived Anonymity.

Online Information Privacy Concerns

In our model, Online Information Privacy Concerns (PRIV) is a multi-dimensional variable that includes collection, unauthorized secondary use, control and general online information privacy concerns. According to Xu et al. (Xu et al., 2011), privacy concerns as a construct is most appropriate because of the "complexity and inconsistencies" in defining and measuring privacy and also because of the reliance on cognitions and perceptions, rather than rational assessments in measuring privacy.

Transparency

Transparency, in our model, refers to the knowledge that the consumer has as to how their personal information will be collected and used. More broadly, it refers to companies' data usage policies. According to Malhotra et al. (2004), the Internet Users Information Privacy Concerns (IUPIC) framework refers to transparency as awareness and defines it as having an understanding of data collection and use practices of an organization. Further, it refers to "the degree to which a consumer is concerned about his/her awareness of organizational information practices" (Culnan, 1995; Foxman & Kilcoyne, 1993; Malhotra et al., 2004: 339). The IUIPC (Malhotra et al., 2004) framework suggests that an awareness of an organization's privacy policies has an impact on their reactions to online privacy threats, and in this case, perceived creepiness.

Control

Control is having the ability to determine how one's personal information is collected and used. It can also refer to the ability to opt-out of a company's data collection, use and sharing practices. Being able to control the collection, use and sharing of one's data may thwart any perceptions of creepiness. If one has control over how their information is used, then unexpected or surprising uses of information don't readily occur since the consumer is in control over the use of their data.

Anonymity

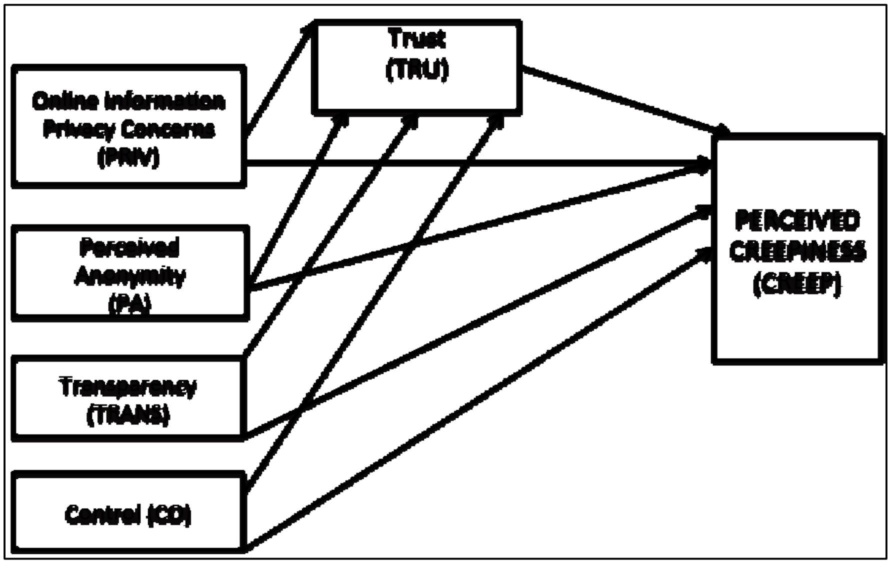
Much of the literature on perceived anonymity centers on how individuals present themselves, relate and share information within online communities (Barth, Datta, Mitchell, & Nissenbaum, 2006; Christopherson, 2007); therefore, making it relevant to our research. When online, many users may believe that their identity is unknown until they receive a communication or ad that "seemingly" knows them.

Trust

In addition to the factors that we identified as variables leading to perceived creepiness, we added the construct of consumer-firm trust to our model to determine the impact it has on perceived creepiness and the independent variables. While there are multiple definitions of trust depending on the context, for our study we will use the definition espoused by Hosmer (1995): trust is one party's (*consumer/Internet user*) optimistic expectation of the behavior of another (*firm*), when the party must make a decision about how to act under conditions of vulnerability and dependence. Trust has also been described as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Lewicki, McAllister, & Bies, 1998: 439; italics my own; Mayer, Davis, & Schoorman, 1995: 712).

Our research model, which shows the relationship of the constructs used in this study, is shown in Figure B1. Since there is not a unified theory of creepy to explain perceived creepiness in the context of personalized communication, we look to privacy, communication and marketing theories to help in our understanding of perceived creepiness.

Figure B1. Research Model



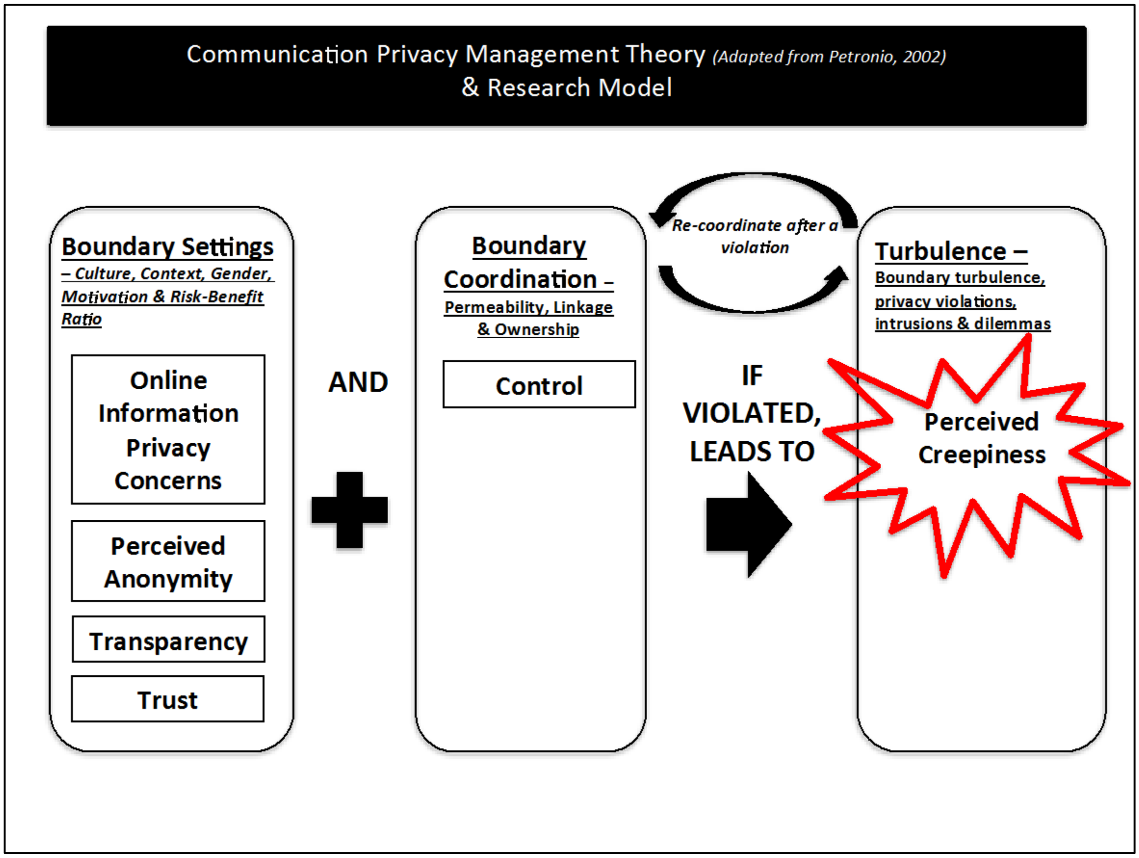
Communication Privacy Management Theory (CPM)

Communication Privacy Management Theory (CPM) (Petronio, 2010) is perhaps the best theory to encapsulate the variables presented in our research model. CPM is an evidence, rule-based system that was constructed to “address the way people manage private information from a communicative perspective” (Petronio, 2002: 176). It also provides a framework for understanding how people manage the disclosure and privacy of information. The essence of CPM is based on the disclosure of personal information and the discloser of the information having some control over what, how and to whom the information is disclosed. At the root of personalized communication and data-driven marketing is personal information. However, most often, while online, personal information is often obtained by the online company in a manner that is not directly disclosed by the subject of the personal information but by other means such as tracking, online behaviors, and surveillance.

CPM is predicated on boundary setting conditions where the individual determines what information to disclose based on five criteria: 1) Cost-benefit ratio – weigh the advantages or disadvantages of disclosing personal information; 2) Context – to whom information is disclosed and why the information is disclosed; 3) Motivations – disclose more to people we know or trust; 4) Gender – men and women disclose personal information differently; and 5) Culture – some cultures value privacy more so than others (Petronio, 2002). After the information has been disclosed, the individual disclosing the data and the recipient of the data act upon three boundary coordination rules: 1) Permeability – how much personal information can be disclosed; 2) Ownership – who can pass this information to 3rd parties; and 3) Linkage – who else may be privy to the disclosed information (Professorgrossman.com & Inter-Act, n.d.). In the CPM framework, boundary turbulence can occur when there is a disconnect between the discloser of the data and the recipient of the data as it pertains to the coordination of the boundary rules. When turbulence occurs, individuals' privacy concerns increase. Figure B2 shows our research model overlaid with the Boundary Setting and Boundary Coordination principles of CPM. We posit that a personalized communication perceived to be creepy would qualify as boundary turbulence as it violates boundary rules of permeability, ownership, and linkage. After boundary turbulence has occurred, the actors must readjust and re-coordinate the boundary rules.

The Communication Privacy Management framework provides a lens to understand perceived creepiness within a marketing context when personal information is the basis for the communication or advertisement. Without a defined theory of creepy that discusses possible determinants of perceived creepiness, CPM helps to explain how one can perceive a communication to be creepy because of the belief that they no longer have control over how their personal information is collected and used (boundary coordination rules). Not knowing nor having control over how one's personal information is collected and used enables an online company to collect and use personal information in unsuspecting and surprising ways, thus invoking boundary turbulence—perceived creepiness.

Figure B2. CPM Theory & Research Model


Communication Privacy Management Theory (Adapted from Petronio, 2002)
& Research Model
Boundary Settings
– Culture, Context, Gender, Motivation & Risk-Benefit Ratio
Online Information Privacy Concerns
Perceived Anonymity
Transparency
Trust
AND
Boundary Coordination –
Permeability, Linkage & Ownership
Control
Re-coordinate after a violation
IF VIOLATED, LEADS TO
Turbulence –
Boundary turbulence, privacy violations, intrusions & dilemmas
Perceived Creepiness

Hypotheses

To test whether the factors identified do lead to perceived creepiness, we have hypothesized the direct effects of our independent variables on trust and perceived creepiness, along with the mediating effect of trust and the moderating effects of age and gender.

Online Information Privacy Concerns

Most often, online information privacy concerns are measured from the perspective of beliefs, attitudes and perceptions (Xu et al., 2011). There have been many studies (Chellappa & Sin, 2005; Culnan, 1993; Dinev et al., 2008; Dinev & Hart, 2004, 2006; Malhotra et al., 2004; Smith et al., 1996; Van Slyke, Shim, Johnson, & Jiang, 2006) where privacy concerns were used as an antecedent to explain behavior-related variables. The studies, in general, conclude that a consumer's concern for privacy impact their behaviors while online in some capacity, which manifests as protecting the amount of information they disclose and the degree to which they engage with online companies (Dinev et al., 2008). We gleaned key dimensions from several frameworks that embody consumer online information privacy concerns, namely: CFIP – Concern for Information Privacy (Smith et al., 1996), IUIPC – Internet Users Information Privacy Concerns (Malhotra et al., 2004), and MUIPC – Mobile Users Information Privacy Concerns (Xu et al., 2012). The purpose of CFIP is to reflect individuals' concern about organizational privacy practices; the purpose of IUIPC was to communicate Internet users' concern for information privacy and MUIPC reflects mobile users' concern for information privacy. While each has a slightly different focus, all of the frameworks deal with the most common information privacy concerns: collection, use, transparency, and control. Since consumers' concern for information affects their online behaviors, we suppose that the same concerns for privacy impact the emotions that are triggered when the information that they have disclosed have been used in an unsuspecting manner to deliver personalized communications and tailored customer experiences, thus:

Hypothesis 1a. Online Information Privacy Concerns has a positive effect on Perceived Creepiness

Hypothesis 1b. Online Information Privacy Concerns has a positive effect on Trust

Hypothesis 1c. The positive effect Online Information Privacy Concerns has on Perceived Creepiness is partially mediated by Trust

Perceived Anonymity

Perceived anonymity is the idea that one's identity is unknown when online. Many consumers perceive that they are anonymous when browsing or searching the Internet, especially if they have not disclosed any personal information to the website that they are visiting. However, the perception of anonymity is diminished when consumers move from one site to another and things that they have searched for appear on an unrelated site sometimes several days later or when a personalized communication or ad is received and is based on information not previously provided by the consumer to the firm sending the communication. Consumers then become aware that they were not as anonymous as they thought. However, it becomes apparent that information was collected about them unknowingly and presented in such in a way that the consumer felt or believed identified them in some way by their location, IP address, their behaviors, likes, dislikes, or some other data element that revealed their identity. These occurrences lead consumers to wonder, "How did they know to show me that ad?" When this occurs, consumers experience that uncanny feeling that they are not as anonymous as they once thought, therefore,

Hypothesis 2a. Perceived Anonymity has a positive effect on Perceived Creepiness

Hypothesis 2b. Perceived Anonymity has a positive effect on Trust

Hypothesis 2c. The positive effect of Perceived Anonymity has on Perceived Creepiness is partially mediated by Trust

Transparency

Transparency is another construct that is tantamount to understanding perceived creepiness and has been widely studied across multiple disciplines with each providing a slightly different lens as to what transparency is and how it is operationalized. However, at the core of the myriad of definitions, transparency is being open and honest. Dapko defines transparency as “the extent to which a stakeholder perceives a firms’ conduct is open and forthright regarding matters relevant to the stakeholder” (Dapko, 2012: 1). Eggert and Helm define transparency “as an individual’s subjective perception of being informed about the relevant actions and properties of the other party in the interaction” (Eggert & Helm, 2003: 101).

If a consumer not only has control over their data and is also made aware by the company of their data usage policies detailing how their data will be collected and used, perceptions of creepiness are lessened as the surprise factor, which is an aspect of creepy, is nullified. We have included transparency within our model as we suggest that transparency can play a role in dispelling perceived creepiness, thus:

Hypothesis 3a. Transparency has a negative effect on Perceived Creepiness

Hypothesis 3b. Transparency has a positive effect on Trust

Hypothesis 3c. The positive effect of Transparency has on Perceived Creepiness is partially mediated by Trust

Control

Control also plays a role in understanding perceived creepiness. Often, privacy is defined in terms of control (Culnan, 1993; Westin, 1967). Having control over how one's personal information is collected and used is a common theme when speaking about personal data and privacy. Having the ability to control what information is shared, with whom, and under what circumstances, is paramount in maintaining privacy and safeguarding one's personal information. A recent Pew Research Study (2014) stated that 91% of adults in the United States feel as though consumers have lost control over how their personal information is collected and used by companies. However, when online, the consumer has minimal control over the collection and use of their data because of various tracking and monitoring tools that are in place to capture consumer behaviors. As unintended uses of data are more prevalent when the consumer loses control over how their data is collected and used, perceptions of creepiness are more likely to occur when personal information is unknowingly used to create personalized communications. Conversely, as consumers have control over the collection and use of their personal information, they will be less inclined to be "creeped out" because they would know what personal information that they have disclosed and, specifically, what and how the information will be used, which would negate unauthorized secondary use, thus:

Hypothesis 4a. Control has a negative effect on Perceived Creepiness

Hypothesis 4b. Control has positive effect on Trust

Hypothesis 4c. The positive effect Control has on Perceived Creepiness is partially mediated by Trust

Trust

In extant literature, trust has been studied from various perspectives; however, the focus of our research is consumer–firm trust. Much has been said about trust, specifically consumer–firm trust (Doney & Cannon, 1997; Sirdeshmukh, Singh, & Sabol, 2002) in buyer–seller as well as in marketing relationships. Further emphasis is on online trust, as it is a key driver of web success and impacts a consumers' willingness to engage and transact online (Beldad, De Jong, & Steehouder, 2010; Urban, Amyx, & Lorenzon, 2009). If a consumer trusts a company and believes that they will act in a trustworthy manner as it pertains to their data and personal information, it may be that a personalized communication may not be perceived to be creepy because there is a belief that that the firm would act in the best interest of the consumer and not engage in activities that would betray their trust. Therefore, we posit that receiving a personalized communication or ad from a trustworthy company would have an impact on the degree to which the communication is perceived to be creepy. Thus, overall:

Hypothesis 5. Trust has a negative effect on Perceived Creepiness

Previous studies of demographics and their impact on Internet users' information privacy concerns suggest that age (Zukowski & Brown, 2007) and gender (Kehoe, Pitkow, & Morton, 1997) (Nowak & Phelps, 1992; Sheehan, 1999; Westin, 1997) does have an impact on one's perception of privacy and what constitutes privacy-invasive activities or behaviors. Since privacy and perceived creepiness are related, it is hypothesized that these variables will also have a similar effect on perceived creepiness.

Gender

There have been several studies (Herring, 1994; Kehoe et al., 1997; Roper Center for Public Opinion Research, 1998; Witmer & Katzman, 1997) on gender and the Internet. It has been shown that men and women interact with the Internet differently (Petronio, 2002). Kehoe et al. (1997) concluded that women are more concerned about online privacy than men. In Sheehan’s (1999). study, the specific focus was on gender differences in attitudes and behaviors toward marketing practices involving information gathering and privacy on-line, to which it was also concluded that women are more concerned about their online privacy in e-commerce situations than men; therefore:

> *Hypothesis 6. The direct effect of Online Information Privacy Concerns on Perceived Creepiness will be positive and stronger for females than for males.*

Age

In 2001, Prensky coined the terms *digital native* and *digital immigrant* (Prensky, 2001). Prensky defines a digital native as a person, typically less than thirty-three years old, who was born into the Digital Age and has grown up with technology and exudes efficacy as it pertains to technology, the Internet, and all things characteristic of the Digital Age. He goes on to say that they are “native speakers” of the digital language. Being a digital native is not so much about what you do, but who you are in terms of the way you relate to technology and the role it plays in your life. On the other hand is the digital immigrant who is typically over thirty-four years old and has had to learn technology as technology was not a regular part of their daily life. Like all immigrants, digital immigrants have to learn how to adapt to their new environment, learn the language and navigate their new surroundings. Prensky also suggests that these distinctions remain in place over time despite how socialized the digital immigrant may become to their digital environment. Although these terms may not be as relevant from a practical perspective as digital technology is more user-friendly and an integral part of most peoples' daily life, for purposes of our research it enables us to ascertain whether those who may be more familiar with how the Internet works as it pertains to search engines, cookies and other tracking software perceive creepiness in a different manner than those who may not be as Internet savvy and have had to learn the digital landscape.

> *Hypothesis 7. The direct effect of Online Information Privacy Concerns on Perceived Creepiness will be positive and stronger for Digital Immigrants (typically those older than 33 years old) than for Digital Natives (typically those younger than 34 years old).*

In our study, we controlled for Internet usage (which includes how long a person has been an Internet user and the amount of time spent online) and online shopping experience (which includes how long ago the first online purchase was made as well as the number of online purchases made on a monthly basis) because the more familiar a person is with the Internet, their perceptions of creepiness may dissipate as the surprise factor and unexpected uses of data is familiar.

Research Design & Methods

Construct Operationalization

In our model, there were six constructs used in our study: Online Information Privacy Concerns, Transparency, Perceived Surveillance, Perceived Anonymity, Trust and Perceived Creepiness. To test our model, we chose to use survey methodology as we felt it was the most appropriate method for measuring perceptions and beliefs without being subject to reporting bias. Additionally, this method allowed us to capture a broader sample in a convenient and inexpensive manner, thus making our results more generalizable than perhaps a lab experiment or another quantitative method. We mostly adapted existing scales to fit our research by changing the wording to reflect online companies as the primary actor in the questions and incorporated personal data or information as the primary subject of our inquiry. Due to the close relationship between perceived creepiness and privacy and our belief that consumers tend to respond to both in a similar manner, we sometimes substituted perceived creepiness for privacy. In Table B1, we provide key information on the scales along with a couple of questions from each construct. To further explore perceived creepiness, we developed three scenarios specifically for this research and asked the respondent to rate the degree of creepiness.

Table B1. Overview of Scales

Construct	Number of Items	Scale	Source	Sample Questions	
Online Information Privacy Concerns (PRIV) – Multi-dimensional construct	15	7-point Likert Scale with “strongly disagree” to “strongly agree”	[redacted]	[redacted]	[redacted]
Collection	5	7-point Likert Scale with “strongly disagree” to “strongly agree”	CFIP – Smith et al., 1996	I'm concerned that social networking sites such as Facebook, LinkedIn and Twitter are collecting my personal information	It bothers me to give personal information to online companies.
Use	3	7-point Likert Scale with “strongly disagree” to “strongly agree”	CFIP – Smith et al., 1996	It bothers me that online companies may use my personal information for other purposes without my permission	It bothers me that online companies share my personal information with other companies without my permission
Control	4	7-point Likert Scale with “strongly disagree” to “strongly agree”	Privacy Control - Xu et al, 2011	I believe I have control over what personal information is shared by online companies.	I believe I can control who can access my personal information after it is collected by online companies.
General	3	7-point Likert Scale with “strongly disagree” to “strongly agree”	CFIP – Smith et al., 1996	I wish my personal information was not so easily accessible to online companies	Compared to other people I know, I am more sensitive about the way online companies handle my personal information.
Transparency (TRANS)	6	7-point Likert Scale with “strongly disagree” to “strongly agree”	4 questions - IUPIC – Subscale - Transparency Malhotra, Kim and Agarwal, 2004; 2 questions - Hustevdt and Kang 2013	I believe that online company's consumer data collection and use policies are readily accessible	It is very important to me that I am aware and knowledgeable about how my personal information will be used by online companies.
Perceived Anonymity (PA)	5	7-point Likert Scale with “strongly disagree” to “strongly agree”	4 questions – Bates & Cox, 2008; 1 question – Pew Research, 2013	Others cannot connect my identity to my online activity.	I feel confident that there is no way to specifically link my online activity to me

Construct	Number of Items	Scale	Source	Sample Questions	
Perceived Surveillance (PS)	4	7-point Likert Scale with “strongly disagree” to “strongly agree”	MUIPC – Xu et al., 2012	I believe that as a result of my using the Internet, information about me that I consider private is being tracked by online companies	It bothers me that online companies are following me on the Internet
Trust (TRU)	5	7-point Likert Scale with “strongly disagree” to “strongly agree”	3 questions – Jarvenpaa & Tractinsky, 1992; 2 questions – Developing & Measuring Trust Measures for E-Commerce – McKnight et al., 2002	I trust online companies to be honest with me when it comes to using my personal information.	Online companies act in my best interests when dealing with my personal information
Unsolicited Marketing Communication	9	One Dimension	Ad Intrusiveness Scale – Li, Edwards & Lee, 2002	Good	Surprising
Perceived Creepiness	8	5-point Likert Scale anchored with “not at all creepy” to “creepy”	4 questions – Self Developed; 4 questions – Privacy Intrusion – Xu et al., 2008	I think personalized ads that collect and use my personal information without my knowledge are unsettling.	I feel threatened when online companies collect and use my personal information for unsolicited advertisements when I did not provide it for that purpose.

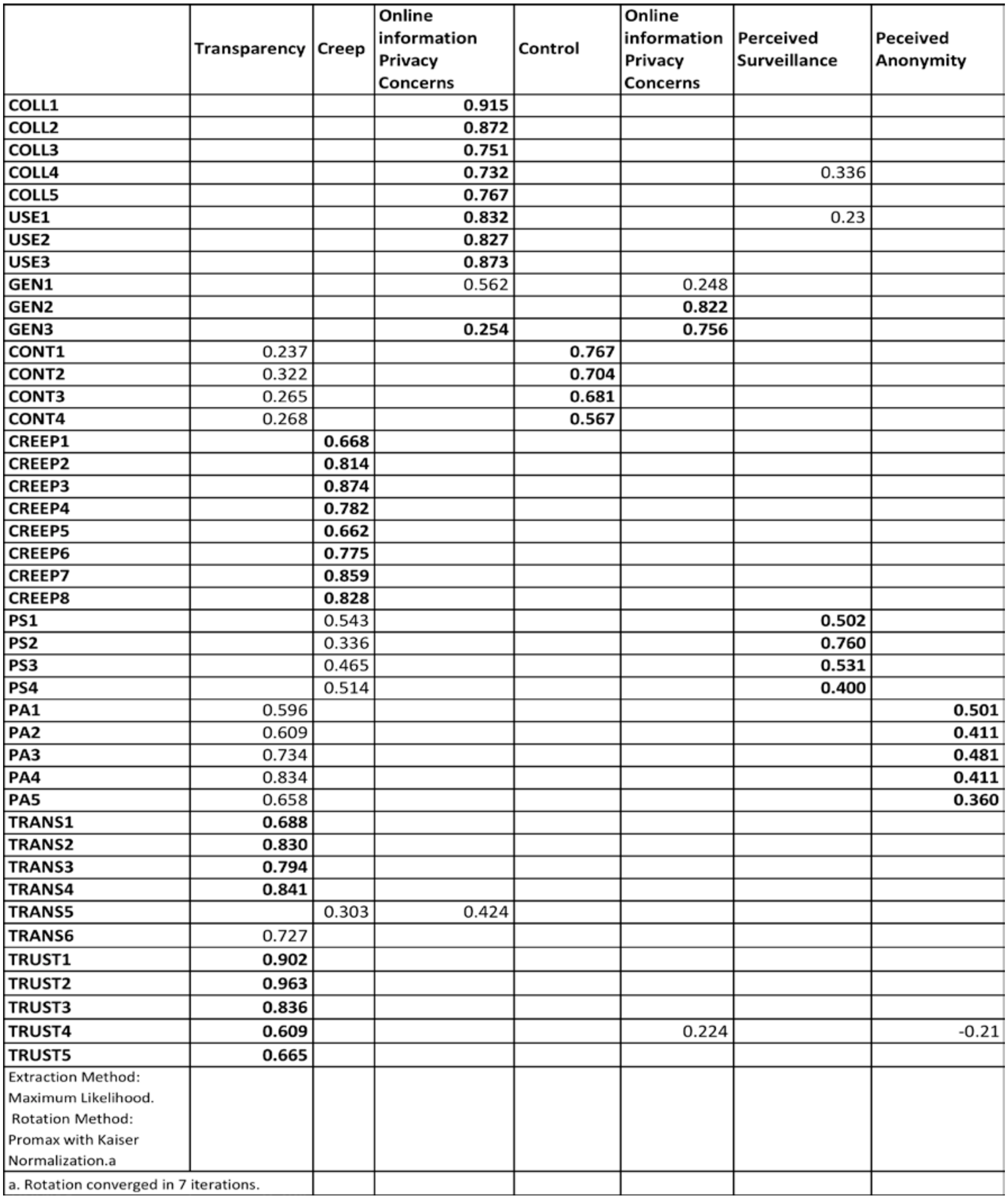
Instrument Development and Validation

After our survey was crafted, we conducted multiple pre-tests before we launched the final survey. The first pre-test was a talk-aloud exercise to ensure that the questions were readable, made logical sense, and that the essence of what we were trying to capture was being asked appropriately. Based on feedback from four participants, we reworded a few questions for clarity. For example, we changed the statement, “I am concerned that online companies may use my personal information for other purposes without my permission” to “It bothers me that online companies may use my personal information for other purposes without my permission.” In another statement, the word “concerns” was replaced with “worries”. To the extent possible, statements that contained the word “concerned” were changed. Since we were trying to understand the emotion surrounding the statements, we used words that connote more emotion. Another example was the rewording of the statement, “Compared to others…” which was changed to “Compared to other people I know…” We made this change to make the statement more personal. It would be more difficult to ascertain “others” in a broad sense compared to the respondent’s circle of affiliations. Additionally, we provided definitions to ensure there was no ambiguity in the terminology being used. We provided definitions for Online Companies, Transparency, and Personal Information, as these terms are sometimes open to interpretation.

Additionally, five people participated in a Q-sort test to ascertain whether forty-two of the statements in the survey were actually aligned with the constructs that were being studied. From this test, 83% (35) of the statements had greater than a majority (60%) agreement, with 20 of those statements showing 80% or higher agreement on the alignment of the statements to the constructs. For the seven statements that did not have a majority agreement, one statement was moved from the Online Information Privacy Concerns construct to Perceived Anonymity, as that was the construct that received the most responses and seemed to be a better fit. There were no additional changes from the original constructs for the other five statements as the original construct seemed most appropriate as they were mostly adapted from existing scales. Also, since we had planned on running a pilot test, we would ascertain how those statements would perform and make any additional adjustments at that point.

Given that perceived creepiness has not been studied in the manner in which we are researching, we wanted to conduct a pilot test to determine if perceived creepiness is a valid construct and also determine if privacy and perceived creepiness are discriminant, despite the relatedness of the constructs. Further, we wanted to test if there was convergent and discriminant validity within and among the other constructs. We conducted a pilot test primarily using Amazon's Mechanical Turk marketplace. There were 154 respondents in our initial pilot. We conducted an exploratory factor analysis (EFA) and were able to determine that one of our constructs (Perceived Privacy Invasion) was not discriminant from perceived creepiness because of cross-loadings of the two constructs. Based on that information, we eliminated the Perceived Privacy Invasion construct and combined the statements with those in the Perceived Creepiness construct since it is the focus of our study. We then conducted another pilot with 145 respondents, which included this revision. The Kaiser-Meyer-Olkin (KMO) Measure of Adequacy was .885 and Bartlett's Test of Sphericity was 4564.288 with 903 degrees of freedom, which was significant at the .000 level, both of which were good indications that the appropriateness of our data was sufficient. The primary purpose of the pilot was to ensure that the Creepy construct was strong since this was a new construct that had not been tested. Since understanding perceived creepiness and the creepy construct was the primary goal of the study, we did not test other measures that would have provided additional information on the viability of our model. This pilot test demonstrated convergence within the perceived creepiness construct and loadings for perceived creepiness ranged from .668–.859. All of the other constructs were discriminant as evidenced by the EFA, except for Transparency and Trust where there were cross-loadings. Aside from those constructs, the cross-loadings of the factors were less than .30 (Hair, Black, Babin, Anderson, & Tatham, 2009) and were convergent within the construct. We proceeded with the model where we would determine if the results for Transparency and Trust would be the same with a larger sample size. Overall, the Trust construct loaded more strongly than Transparency. This was acceptable since Trust was going to be the mediating variable within our model. The EFA also showed that the seven factors explained 73% of the variance. The pattern matrix for the pilot test is shown in Table B2. No further analysis was performed on either pilot test.

Table B2. Pattern Matrix – Pilot Test



	Transparency	Creep	Online information Privacy Concerns	Control	Online information Privacy Concerns	Perceived Surveillance	Peceived Anonymity
COLL1			**0.915**				
COLL2			**0.872**				
COLL3			**0.751**				
COLL4			**0.732**			0.336	
COLL5			**0.767**				
USE1			**0.832**			0.23	
USE2			**0.827**				
USE3			**0.873**				
GEN1			0.562		0.248		
GEN2					**0.822**		
GEN3			**0.254**		**0.756**		
CONT1	0.237			**0.767**			
CONT2	0.322			**0.704**			
CONT3	0.265			**0.681**			
CONT4	0.268			**0.567**			
CREEP1		**0.668**					
CREEP2		**0.814**					
CREEP3		**0.874**					
CREEP4		**0.782**					
CREEP5		**0.662**					
CREEP6		**0.775**					
CREEP7		**0.859**					
CREEP8		**0.828**					
PS1		0.543				**0.502**	
PS2		0.336				**0.760**	
PS3		0.465				**0.531**	
PS4		0.514				**0.400**	
PA1	0.596						**0.501**
PA2	0.609						**0.411**
PA3	0.734						**0.481**
PA4	0.834						**0.411**
PA5	0.658						**0.360**
TRANS1	**0.688**						
TRANS2	**0.830**						
TRANS3	**0.794**						
TRANS4	**0.841**						
TRANS5		0.303	0.424				
TRANS6	0.727						
TRUST1	**0.902**						
TRUST2	**0.963**						
TRUST3	**0.836**						
TRUST4	**0.609**				0.224		-0.21
TRUST5	**0.665**						
Extraction Method: Maximum Likelihood. Rotation Method: Promax with Kaiser Normalization.a							
a. Rotation converged in 7 iterations.							

The final survey contained twenty-one questions, eight of which were directly related to our constructs along with three scenarios in which the respondents were to assess the degree of perceived creepiness; six questions were asked to understand Internet usage and activities performed using the Internet and three demographic questions were asked to garner age, gender and highest educational level obtained. Since we measured our independent and dependent variables within the same instrument, it was necessary to assess Common Method Bias (CMB). To test CMB, it is most appropriate to use a marker variable; therefore, we included a social desirability scale. A social desirability scale was selected because we assert that there is a socially desirable way to answer questions about emotions, beliefs and confidence for which we measured to some degree within the Perceived Anonymity and Online Information Privacy Concerns constructs. Our final survey can be found in Appendix B1.

Data Collection and Sampling

We collected data between February and March 2015 through several channels: Mechanical Turk (MTurk), social media and the personal and professional network of the co-investigator. Mechanical Turk is an Internet crowdsourcing marketplace where requestors post jobs to complete called a HIT (human intelligence task), and workers choose the HITs to complete for a small fee. Mechanical Turk has increased in popularity and usage among social science researchers because of its ability to get high-quality data rapidly and inexpensively (Burhmester et al., 2011). In a study on the viability of Mechanical Turk and the quality of data received, it was stated that using Turkers, a term referred to those completing task in Mechanical Turk are just as valid and reliable as traditional research methods (Burhmester et al., 2011). One of the benefits of Mechanical Turk is the diversity of the respondents, which Burhmester et al. (2011) found to be more diverse than college students who are often used in research studies. This is particularly helpful in this study as we were able to capture a cross-section of varied demographics that may not exist within the researchers' personal and professional network. We received 338 responses from Mechanical Turk, representing 81% of our sample data.

The online survey host was Qualtrics, which sent 334 emails to the personal and professional network of the co-investigator, of which 126 were opened, yielding an open rate of 38%; of those opened, 47% of 59 surveys were completed. Based on a study by Silverpop, the average open rate for email marketing messages within the US is 20.1%.[16] While our email is not a marketing message per se, this measure provides us with insight as to how our results compare to mainstream email marketing messages. According to Fluid Surveys University, the average response rate for online surveys to the general public is 24.8%[17] which is in line with (Sheehan & Hoy, 1999b) study on email survey response rates that reported the response rate to be 24% in 2000. Our survey was in line with baseline open and response rates for email surveys. Total email responses represented 14% of our sample data. Lastly, the survey was posted on LinkedIn and Facebook, which garnered 21 responses, equating to 5% of our sample data.

In total, our survey generated 418 responses. Surveys that were less than 50% complete were eliminated, resulting in 389 valid responses. Since MTurk completed over 80% of the surveys within seven days, we did not have wave phenomena; therefore, we did not do a wave analysis to measure wave invariance. Demographic information including the age, gender, and highest educational level achieved of the respondents is displayed in Table B3. Most notable is that 55% of the respondents were male and 45% were female. Median age was 37 years old and 61% had attained a Bachelor's, Master's,

[16] http://idma.ie/wp-content/uploads/2014/05/Email-Marketing-Metrics-Benchmark-Study-2014-Silverpop.pdf

[17] http://fluidsurveys.com/university/response-rate-statistics-online-surveys-aiming

Professional or Doctorate degree. Eighty-five percent of the respondents spend 40 hours or less online excluding email and work related activities, and 73% of the respondents have been Internet users between eleven and twenty years.

Table B3. Demographics Summary of Our Sample

Item		Number	Percentage
Gender (N=389)	Male	213	55%
	Female	175	45%
	Not Reported	1	0%
Age (N=389)	18 - 27 (Millinieals)	72	19%
	28 - 43 (Gen X)	195	50%
	44 - 62 (Baby Boomer)	110	28%
	63+ (Traditionalist)	8	2%
	Not Reported	4	1%
Education Level (N=389)	Some high school; No Diploma	3	1%
	High School Graduate	91	23%
	Associates Degree	58	15%
	Bachelor's Degree	148	38%
	Master's Degree	73	19%
	Professional Degree	7	2%
	Doctorate Degree	8	2%
	Not Reported	1	0%
Internet Usage (N=389)	0 - 5 Years	6	2%
	6 - 10 Years	41	11%
	11 -15 Years	126	32%
	16 - 20 Years	160	41%
	Over 20 Years	53	14%
	Not Reported	3	1%

Measurement Model

Data screening. The analysis of my data began with examining the data set to ensure all items and constructs were represented, assess any missing values as well as perform other univariate measures. Visual examination of our results confirmed all items and constructs were present. I completed a missing data analysis, and fifty-one of the ninety-three items were missing data; forty-eight of the fifty-three items were missing between one and four values. Items Q11-1, Q11-2 and Q11-3 all belonging to the same construct, Online Privacy had 15 missing values. None of the missing values represented more than 5% of the sample size; therefore, all missing values were given the mean of all available values for that particular item.

Demographic as well as Internet usage questions also had missing data. Missing data was also well below 5% of the sample size. No values were imputed and are shown as “not reported” in our demographic summary as shown on Table B3.

Outliers and normality. All construct items were based on ordinal scales; therefore, no outliers exist. Since we used Likert scales, we had no expectations of skewness and therefore, did not test for skewness. However, we did test the normality of our data by determining if kurtosis was present. We identified two items (Priv1 – 3.088 and Coll - 2 3.485) that exceeded the acceptable threshold of kurtosis for large samples between -2.58 and +2.58 according to Hair et al. (2010). Since Priv1 is around 3.0 it will be retained, but flagged to review for potential issues in subsequent analysis; Coll 2 was dropped from the data set.

To measure our model we performed an exploratory factor analysis (EFA), a confirmatory factor analysis (CFA) and finally a structural equation model (SEM) analysis.

Exploratory factor analysis**.** The purpose of the EFA was to help determine if the observed variables performed as we had originally anticipated were correlated and also to determine if the minimum criteria of reliability and validity were met. We used the Principal Components Analysis extraction method along with Promax rotation method as it is suitable for large datasets and can account for correlated factors. Following Hinkin's (1998) recommendation, the following criteria were used to determine the number of factors: eigenvalue greater than one, scree plot examination and percentage of variance explained (Cattell, 1966). We also examined factor loadings, cross-loadings and communalities. We reviewed the communalities to determine if they met the suggested threshold, which should be above .3 (Dziuban & Shirkey, 1974). Items were retained if they had high loadings on their primary factor or low cross-loadings on another factor. Using this criteria, we eliminated one construct: Collection/Use which contained eight items, four items (PS1 – PS4) representing Perceived Surveillance, one item (PRIV1) from Online Information Privacy Concerns and three items (TRANS1, TRANS2 and TRANS6) from the Transparency construct.

Adequacy, reliability and validity measures. We addressed the adequacy, reliability and validity measures for the final six-factor model. To assess adequacy we reviewed the Kaiser-Meyer-Olkin (KMO) and the Bartlett's Test for Sphericity. KMO was .912 and the Bartlett's Test for Sphericity was significant at .000 level (Chi-square = 8246.136, df = 325, p = 0.000). We also examined Measures of Sampling Adequacy

(MSA) across the diagonal of the anti-image matrix to ensure that they were above .70 (Dziuban & Shirkey, 1974), of which they were; values ranged from .743 to .964. The reproduced matrix showed 9% non-redundant residuals greater than 0.05 (Fornell & Larcker, 1981). While this is over the accepted threshold, the other adequacy measures are strong; therefore, we believe our model to be adequate. Reliability and validity measures would further test the strength of our model.

Reliability was measured by Cronbach's Alpha for the six factors within our model to ensure that they met the recommended level of 0.70 (Nunnally, 1978). Cronbach's Alpha for the overall model was .824. Cronbach's Alpha for the individual constructs exceeded the threshold as well. Table B4 shows the Cronbach's Alpha for all of the constructs. All of the factors within our model are reflective in that their indicators are highly correlated and interchangeable (Jarvis, MacKenzie, & Podsakoff, 2003).

Table B4. Cronbach's Alpha Measure of Reliability

Factor Label	Cronbach's Alpha	Number of Items	Specification
Overall Model	**0.824**	**26**	**Reflective**
Trust	0.925	5	Reflective
Perceived Anonymity	0.914	5	Reflective
Control	0.892	4	Reflective
Online Information Privacy Concerns	0.944	2	Reflective
Transparency	0.908	2	Reflective
Perceived Creepiness	0.936	8	Reflective

We also tested for convergent and discriminant validity by analyzing the factor loadings to ensure that they exceeded the recommended threshold of 0.350 for sample sizes greater than 300 (Hair, Black, Babin, & Anderson, 2010). The Patten Matrix shown in Table B5 reflects convergent validity as all items loaded cleanly on one factor.

Table B5. Pattern Matrix

PATTERN MATRIX	CREEP	TRUST	PERCEIVED ANONYMITY	CONTROL	ONLINE INFORMATION PRIVACY CONCERNS	TRANSPARENCY
CREEP1	0.867					
CREEP2	0.887					
CREEP3	0.821					
CREEP4	0.877					
CREEP5	0.878					
CREEP6	0.802					
CREEP7	0.814					
CREEP8	0.593					
TRUST1		0.791				
TRUST2		0.865				
TRUST3		0.959				
TRUST4		0.91				
TRUST5		0.793				
CONT1				0.917		
CONT2				0.95		
CONT3				0.878		
CONT4				0.705		
PRIV2					0.933	
PRIV3					0.917	
PA5			0.851			
PA6			0.83			
PA7			0.838			
PA8			0.912			
PA9			0.848			
TRANS3						0.942
TRANS4						0.918

NOTE: Extraction Method: Principal Component Analysis.
Rotation Method: Promax with Kaiser Normalization.
Rotation converged in 6 iterations.

Moreover, reviewing the correlation matrix substantiated discriminant validity; there were no correlations above 0.700. Our six-factor model explained 77.5% of the total variance and all extracted factors had eigenvalues over 1.00.

Confirmatory factor analysis (CFA). For our confirmatory factor analysis (CFA), we used AMOS software, a covariance-based structural equation modeling technique where we used the Maximum Likelihood estimation approach. We examined modification indices and analyzed several fit statistics, including chi-square, CFI and RMSEA to ascertain the goodness of fit of our model and to ensure that the measures were within suggested thresholds (Hu & Bentler, 1995; Tabachnick & Fidell, 2007: 715). CFI for our model was .969, which exceeds the recommended threshold of .950, which suggests that the hypothesized model is an adequate fit to the data. Adjusted Goodness of Fit (AGFI) was .88, slightly below the suggested threshold of .90; however, all other fit statistics were within acceptable range.

Table B6 show the results of the goodness of fit measures (Incremental, Absolute, and Statistical) from which we can conclude that the goodness of fit for our measurement model is sufficient.

Table B6. Goodness of Fit Statistics

Goodness of fit statistics	Observed Value	Recommended
Statistical		
Chi-square	539.889	
Degrees of freedom (DF)	284	
CMIN/DF	1.901	Between 1 and 3
p-value	0.000	
Relative		
CFI	0.969	>0.950
Absolute		
SRMR	0.0411	<0.05
RMSEA (90% CI)	0.048	<0.060
RMSEA (Low/High)	.042/.054	
P-Close	0.678	>0.050
AGFI	0.88	>0.90

To establish validity and reliability we used the following measures: composite reliability (CR), average variance extracted (AVE), maximum shared variance (MSV) and average shared variance (ASV). Validity and reliability measures were analyzed based on the standards of Bagozzi and Yi (1988) whereby: 1) CFA factor loadings should exceed .5 (Hair et al., 2010); 2) the composite reliability (CR) should exceed 0.7; and 3) the average variance extracted (AVE) which measures the amount of variance attributable to measurement error, should exceed 0.50 for every construct (Fornell & Larcker, 1981).

To test for convergent validity, AVE was calculated for all factors, and each factor exceeded the recommended threshold of 0.50. The composite reliability CR ranged from .908 to .943, thus exceeding the minimum threshold of 0.70, indicating reliability of our factors. To test for discriminant validity, the square root of the AVE was compared to all inter-factor correlations. Four of the six factors were below .90 (Hair et al., 2010); the other factors were .945 (Online Information Privacy Concerns) and .912 (Transparency). These results are reasonable given that these two constructs have two items, slightly below what is required for a strong construct. However, all constructs meet suggested thresholds for other validity and reliability measures. Table B7 provides a summary of the validity measures and Table B8 shows the AVE (on the diagonal) in comparison to inter-factor correlations.

Table B7. Reliability and Validity Measures

Construct	CR (>0.70)	AVE (>0.50)	MSV	ASV
PRIVACY	0.943	0.893	0.319	0.075
CREEP	0.937	0.650	0.319	0.141
TRUST	0.926	0.717	0.319	0.183
ANON	0.914	0.681	0.425	0.180
CONTROL	0.908	0.718	0.425	0.177
TRANS	0.908	0.832	0.319	0.132
Convergent Validity	**CR >AVE**			
PRIVACY	Yes			
CREEP	Yes			
TRUST	Yes			
ANON	Yes			
CONTROL	Yes			
TRANS	Yes			
Discriminant Validity	**MSV > AVE**	**ASV < AVE**		
PRIVACY	Yes	Yes		
CREEP	Yes	Yes		
TRUST	Yes	Yes		
ANON	Yes	Yes		
CONTROL	Yes	Yes		
TRANS	Yes	Yes		

Table B8. Comparison between AVE and Inter-Factor Correlations

Online Information Privacy Concerns	Perceived Creepiness	Trust	Perceived Anonymity	Control	Transparency
0.945					
0.565	**0.806**				
-0.192	-0.32	**0.847**			
-0.043	-0.331	0.482	**0.825**		
0.002	-0.328	0.472	0.652	**0.847**	
-0.132	-0.257	0.565	0.359	0.359	**0.912**

Common method bias. A single survey was used to collect all of the data for both dependent and independent variables introducing the possibility of common method bias. In order to understand if method bias is affecting the results of the measurement model, we conducted a common latent factor test (CLF) (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Our survey included a social desirability scale, which included five items (Hays et al., 1989) and was used as a marker variable in our CLF test. After visually comparing the standardized regression weights before and after adding the Common Latent Factor (CLF), none of the regression weights were affected by the CLF (greater than 0.20). We found common method bias to be 9%, which is less than the 10% threshold indicating a problem with common method bias (Podsakoff et al., 2003). Additionally, we reviewed the covariance of the social desirability scale with the constructs, and none of the paths were significant. Since we did not have any evidence of common method bias within our study, we imputed the variables without the common latent factor.

Invariance tests. We conducted configural and metric invariance tests for the two categories that were moderated within our structural model: gender and age from the perspective of our respondents being categorized as a digital native (33 years old and younger) or Digital Immigrant (34 years and older) (Presky, 2001). In terms of gender, the model fit of the unconstrained measurement model had adequate fit (cmin/df=2.324; cfi=. 901). To further test for configural invariance, we conducted a chi-square difference test. After constraining the models to be equal, we found that the chi-square difference was not significant (p-value>0.05). The results from these two test demonstrated that the criterion for both configural and metric invariance was met and the groups are invariant.

For the digital native/immigrant category, the unconstrained measurement model had adequate model fit as well (cmin/df=2.318; cfi=. 898), again indicating that the model is configurally invariant. We conducted a critical ratios difference tests with both groups and found one construct (Control) to be somewhat problematic. Two of the items were significant; however, one item (Control4) was significant at the 0.05 level, thus resulting in partial metric invariance. Although the fit statistics for age and gender do not appear very strong, (Hair, Ringle, & Sarstedt, 2013) suggest that other factors such as the number of observations, number of observed variables and sample size may impact the goodness of fit of the model. Taking that into consideration, our goodness of fit measures are adequate.

All of the psychometric properties tested were sufficient, thus allowing further analysis with structural equation modeling (SEM).

Structural model analysis**.** One of the initial tests in our SEM model was testing for multicollinearity of our predictor variables to ensure that all of the variables were discreet. Within IBM SPSS, Tolerance and Variance Inflation Factor (VIF) measure multi-collinearity. According to (Hair et al., 2013)., Tolerance values below .20 and VIF values above 5 indicate multicollinearity issues. Table B9 show the results of our test indicating no multicollinearity issues for each of the endogenous variables within our model as all of the Tolerance values exceeded .20 and VIF values were well below 5.

Table B9. Collinearity Tests Summary

	Collinearity Statistics	
	Tolerance	**VIF**
TRANS	0.661	1.514
PRIV	0.883	1.132
ANON	0.512	1.954
TRUST	0.539	1.854
CONT	0.514	1.944

Our SEM demonstrated adequate fit (cmin/df - 2.872, p-value-.000; cfi - .965). Table B10 summarizes the statistical, relative and absolute fit measures. During our SEM analysis, we also tested the mediating effects of trust between the independent variables and perceived creepiness and multi-group moderation for age and gender while controlling for Internet usage and online shopping experience. Control variables had no significant effect on our dependent variable, perceived creepiness.

Table B10. Goodness of Fit Statistics – SEM

Goodness of fit statistics	Observed Value	Recommended
Statistical		
Chi-square	60.32	
Degrees of freedom (DF)	21	
CMIN/DF	2.872	Between 1 and 3
p-value	0.000	
Relative		
CFI	0.965	>0.950
Absolute		
SRMR	0.0411	<0.05
RMSEA (90% CI)	0.069	<0.060
RMSEA (Low/High)	.049/.090	
P-Close	0.056	>0.050
AGFI	0.926	>0.90

Direct effects. To better our understanding of perceived creepiness, we measured the direct effects of Online Information Privacy Concerns, Perceived Anonymity, Transparency and Control on Perceived Creepiness. Additionally, we tested the endogenous variables on Trust to determine the direct effects of those paths since Trust is a key driver in online engagement between consumers and online companies and consumers' willingness to provide personal information which drives personalized communication (Schoenbachler & Gordon, 2002). A summary of the path analysis of direct effects is shown in Table B11.

Table B11. Path Analysis of Direct Effects

As it Path			Estimate	Standard Error	t-value	P	Significant
TRUST	<---	PRIV	-0.18	0.024	-4.627	0.001	Yes
TRUST	<---	ANON	0.19	0.037	3.757	0.001	Yes
TRUST	<---	TRANS	0.40	0.028	9.648	0.001	Yes
TRUST	<---	CONT	0.19	0.033	3.652	0.001	Yes
CREEP	<---	TRUST	-0.08	0.059	-1.779	0.075	No
CREEP	<---	PRIV	0.44	0.028	11.977	0.001	Yes
CREEP	<---	ANON	-0.23	0.045	-4.693	0.001	Yes
CREEP	<---	TRANS	-0.11	0.036	-2.673	0.008	Yes
CREEP	<---	CONT	-0.22	0.04	-4.543	0.001	Yes

Mediation. To test the mediating effect of trust and transparency, perceived anonymity, privacy and control on perceived creepiness, we utilized the Baron and Kenny (1986) approach, which compares the direct effects with and without mediation. Additionally, we tested mediation significance using 2000 bias-corrected bootstrapping resamples in AMOS. Additionally, we conducted multi-group moderation tests for age and gender using the critical ratios difference test for each path.

Key Findings

Figure B3 provides a visual representation of the direct and mediating effects in our hypothesized model. We next report them separately:

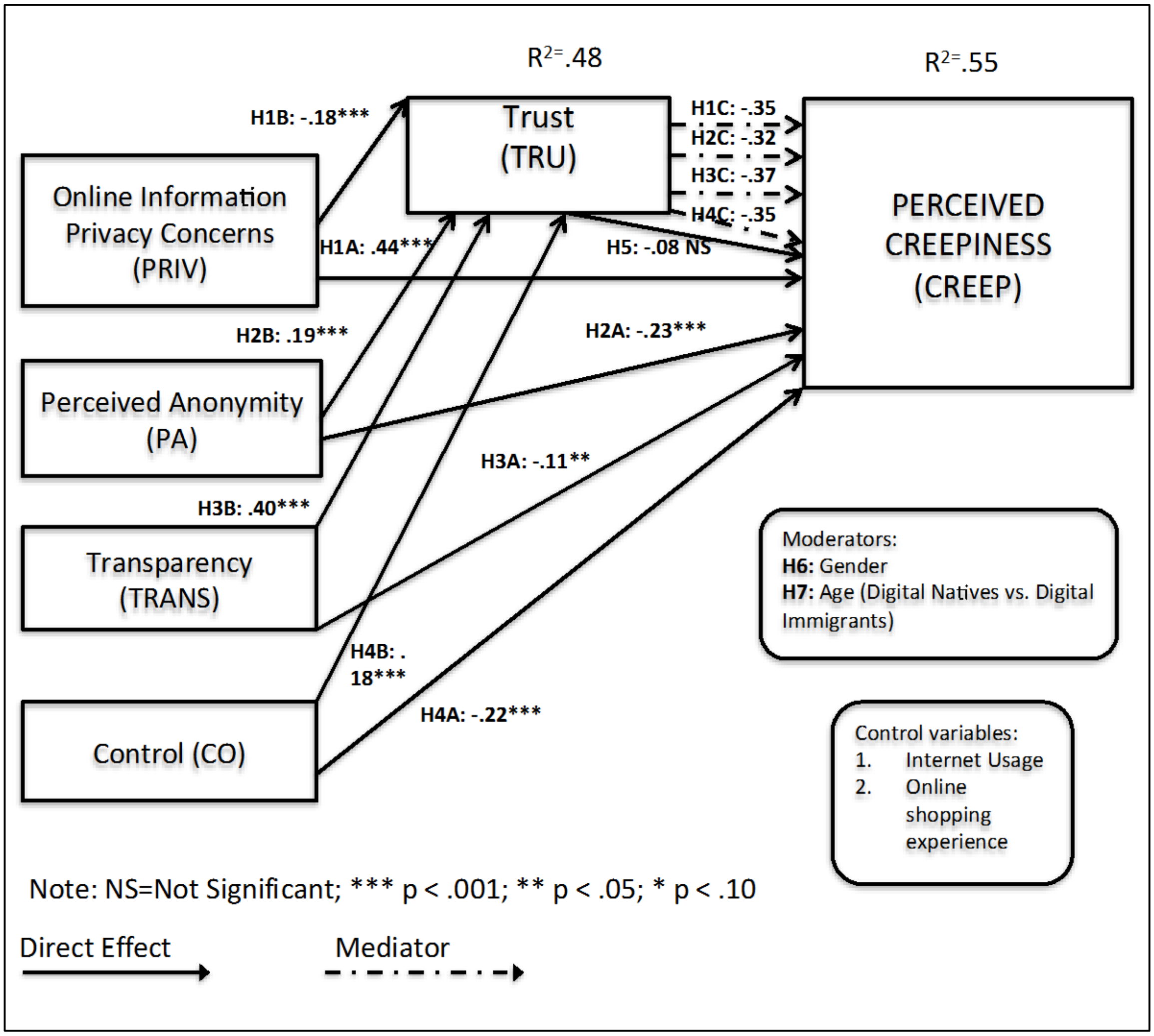
> *Hypothesis 1a. Online Information Privacy Concerns has a positive effect on Perceived Creepiness.* As expected, Online Information Privacy Concerns had a positive direct effect on Perceived Creepiness (0.44, p-value=.001) supporting our hypotheses.
>
> *Hypothesis 1b. Online Information Privacy Concerns has a positive effect on Trust. This hypothesis was not supported; Online Information Privacy Concerns had a negative direct effect on Trust (-0.18, p-value=.001)*
>
> *Hypothesis 1c. The positive effect Online Information Privacy Concerns has on Perceived Creepiness is partially mediated by Trust. Trust partially mediated the relationship between Online Information Privacy Concerns and Perceived Creepiness. Hypothesis supported.*
>
> *Hypothesis 2a. Perceived Anonymity has a positive effect on Perceived Creepiness. Perceived Anonymity had a negative direct effect on Perceived Creepiness (-0.23, p-value=.001). The hypothesis was not supported.*
>
> *Hypothesis 2b. Perceived Anonymity has a positive effect on Trust. Our hypothesis was supported because Perceived Anonymity had a positive direct effect on Trust (0.19, p-value=.001).*
>
> *Hypothesis 2c. The positive effect of Perceived Anonymity has on Perceived Creepiness is partially mediated by Trust. There was no mediation between Perceived Anonymity and Perceived Creepiness. Hypothesis not supported.*
>
> *Hypothesis 3a. Transparency has a negative effect on Perceived Creepiness. As we hypothesized, Transparency had a direct negative effect on Perceived Creepiness (-0.11, p-value=.008). Hypothesis supported.*
>
> *Hypothesis 3b. Transparency has a positive effect on Trust. Transparency had a positive direct effect on Trust (0.40, p-value=.001). Hypothesis supported.*
>
> *Hypothesis 3c. The positive effect of Transparency has on Perceived Creepiness is partially mediated by Trust. Trust was not a mediating factor between Transparency and Perceived Creepiness. Not supported.*
>
> *Hypothesis 4a. Control has a negative effect on Perceived Creepiness. Control had a direct negative effect on Perceived Creepiness; therefore, our hypothesis was supported (-0.22, p-value=.001).*

Hypothesis 4b. Control has a positive effect on Trust. Our hypothesis was supported: Control had a direct positive effect on Trust (0.19, p-value=.001)

Hypothesis 4c. The positive effect Control has on Perceived Creepiness is partially mediated by Trust. Trust partially mediated the relationship between Control and Perceived Creepiness. Supported.

Hypothesis 5. Trust has a negative effect on Perceived Creepiness. Our results showed that Trust had a non-significant negative direct on Perceived Creepiness (-0.08, p-value=.075). Not supported.

Figure B3. Summary of the Results of our Hypotheses



Multi-group Moderation

We found that, for age (Digital Natives/Digital Immigrants), only one path was significant, Online Information Privacy Concerns on Perceived Creepiness (-4.054, P-Value=.01). After conducting a path analysis between males and females, two paths were significantly different; they were Online Information Privacy Concerns and Perceived Creepiness (-1.941, P-Value - .10) and Control and Perceived Creepiness (-.3.851, P-Value - .01). Based on these findings, age (Digital Natives/Digital Immigrants) and gender did not have a significant moderating effect on our model. Table B12 provides a summary of the results of our hypotheses.

Table B12. Summary of Hypothesized Results

HYPOTHESES	EVIDENCE	SUPPORTED
H1A: Online Information Privacy Concerns has a positive effect on Perceived Creepiness	.44 (p=.001)	Yes
H1B: Online Information Privacy Concerns has a positive effect on Trust	-.18 (p=.001)	No
H1C: The positive effect Online Information Privacy Concerns has on Perceived Creepiness is partially mediated by Trust	Direct w/o Med: .453***; Direct w/Med: .438***; Indirect: .050***	Partial Mediation
H2A: Perceived Anonymity has a positive effect on Perceived Creepiness	-.23 (p=.001)	No
H2B: Perceived Anonymity has a positive effect on Trust	.19 (p=.001)	Yes
H2C: The positive effect of Perceived Anonymity has on Perceived Creepiness is partially mediated by Trust	Direct w/o Med: -.243***; Direct w/Med: -.226**; Indirect: .052***	No Mediation
H3A: Transparency has a negative effect on Perceived Creepiness	-.11 (p=.008)	Yes
H3B: Transparency has a positive effect on Trust	.40 (p=.001)	Yes
H3C: The positive effect of Transparency has on Perceived Creepiness is partially mediated by Trust	Direct w/o Med: -.145***; Direct w/Med: -.112**; Indirect: .068***	No Mediation
H4A: Control has a negative effect on Perceived Creepiness	-.22 (p=.001)	Yes
H4B: Control has positive effect on Trust	.19 (p=.001)	Yes
H4A: The positive effect Control has on Perceived Creepiness is partially mediated by Trust	Direct w/o Med: -.231***; Direct w/Med: -.217***; Indirect: .046***	Partial Mediation
H5: Trust has a negative effect on Perceived Creepiness	-.08 (p=.001)	No
H6: The direct effect of Online Information Privacy Concerns on Perceived Creepiness will be positive and stronger for females than for males	Females: 0.284, Pvalue=.000; Males: 0.391, Pvalue=.000, Z-score: -1.941, Pvalue=.10	No
H7: The direct effect of Online Information Privacy Concerns will be positive and stronger for Digital Immigrants (typically those older than 33 years old) than for Digital Natives (typically those younger than 34 years old	Natives: 0.446, Pvalue=.000, Immigrants:0.221, Pvalue=.000, Z-score:-4.054, Pvalue=.01	Yes

Post-Hoc Analysis

In a further attempt to understand perceived creepiness, we developed three fictitious scenarios for our research in which respondents had to rate the degree to which they perceived the scenarios to be creepy. We used a 5-point Likert scale with (1) being "not at all creepy" and (5) being "creepy". While the scenarios were fictitious, they mimic to some degree actual activities that occur when on the Internet, as well as previous reports of perceived creepy activities, such as Zappos shoe ads "following" you on the Internet (Helft & Vega, 2010) and Target knowing a girl is pregnant based on her buying habits. The fact that Target knew so much about their customers' buying habits and about their pregnancies ahead of time "creeped" people out (Hill, 2012).

> *Scenario 1: You search online for information about an upcoming vacation. You visit travel sites to research airfares, airline schedules and hotels for different destinations, but do not book a hotel or flight.*
>
> *Q1: After browsing for vacation information, you visit a social networking site to catch up with your friends. While you are logged on, an ad appears from a travel agency that you were not familiar with for a vacation package for one of the destinations you had just researched.*
>
> *Q2: A couple of days later, you visit an online news site. While you are visiting the news site, an ad appears from the hotel where you are a member of their rewards program. The offer is for one of the destinations you had researched previously.*

This scenario depicts an interaction that does not use sensitive personal information – researching for a vacation. In the first question, the consumer is performing an unrelated task to the vacation search, yet something that was previously researched appears.

The second question infers a relationship between the consumer and a hotel; however, the search was only made to a travel site, not the hotel that served the ad. The objective of this question was to determine if having a relationship with the company, such as being a part of a rewards program would impact the perception of creepiness. There was little difference in the responses, 68.10% felt that question one was somewhat creepy or creepy and 68.40% of respondents felt that question two was somewhat creepy or creepy, perhaps suggesting that having a relationship with the company does not necessarily change the perception of creepiness.

> *Scenario 2: You are experiencing what you believe are flu-like symptoms. You search the Internet on a few health related sites for possible remedies.*
>
> *Q1: Later in the day, you visit the site of an online retailer where you regularly shop to make a purchase. You notice ads appear for cold and flu medication.*
>
> *Q2: The next day while online, ad appears from a local drugstore with a link to receive coupons for cold and flu medication.*

The purpose of this scenario was to depict a more personal issue such as health, which is usually regarded as more sensitive personal information (Bansal & Gefen, 2010). Question one indicates a relationship with an online retailer, although the consumer did not specifically search the retailer's site, as they were on a health related site. In question two, the only relationship is geographical; however, the consumer stands to gain something of value—coupons. For question one, 62.50% felt the personalized message was somewhat creepy or creepy and question two, even when there was something of value to be obtained, 66.80% felt the interaction was somewhat creepy or creepy. Using Social Exchange Theory (Emerson, 1976) as a foundation, Culnan and Bies (2003) introduced the Privacy Calculus, which posits that individuals are willing to forego some measure of privacy in exchange for something of value. In this scenario, the local drugstore is able to take advantage of location-aware marketing (LAM), which targets customers with personalized ads based on their location. According to Xu et al. (Xu & Gupta, 2009) "marketers can utilize this emerging technology to deliver personalized marketing messages based on consumers' geographical location and predictions of their needs, and to reach mobile consumers' through their mobile devices on a geographically targeted basis" (p. 42). While there are upsides to this technology, consumers have not fully embodied this concept due to privacy concerns and in our test, perceived creepiness. The responses to question two seem to support the breach of a social contract where societal norms assume that the online company will safeguard their personal information. In this case, after performing the privacy calculus, the benefit of receiving coupons did not outweigh the perceived risk.

> *Scenario 3: One evening you are on your computer working on a report, when suddenly your computer crashes. The next morning you access your email, and one of your messages is an offer for a discount on a new computer (same brand as the one that crashed).*

This scenario does not involve searching on the Internet, but online activities where communications or advertisements received were based on the consumers' behavior. 85.40% of respondents felt that this personalized communication was somewhat creepy or creepy, perhaps due in part to the fact that no information was directly provided to the company; yet, a seemingly unknown fact appears to be known by the computer company.

In a prior study (Ur et al., 2012), respondents stated that online behavioral advertising was smart, useful, scary and creepy. In our study, we presented participants with eight words and a phrase (Good, Smart, Useful, Scary, Creepy, Relevant, Surprising, Evil and Violation of my Privacy) to describe unsolicited marketing communications and advertisements that use their personal information on a 7-point Likert scale ranging from (1) – Strongly Disagree to (7) – Strongly Agree. The top five words or phrase in which respondents somewhat agree, agree or strongly agree in describing personalized communications were 1.) Violation of privacy (77.90%), 2.) Creepy (73.00%), 3.) Scary (65.30%), 4.) Surprising (43.80%) and Smart (33.00%). Despite Marketers desire to deliver the right message, to the right person at the right time (DoubleClick website, 2010), only 32.40% felt that the communications were relevant, and 10.50% of the respondents felt that personalized marketing communications were good. Table B13 displays the full list of the choices, the response percentage and rank by percentage.

Table B13. Respondents View of Unsolicited Marketing Communications

Item	Percentage (Somewhat Agree, Agree or Strongly Agree)	Rank (By Percentage)
Violation of Privacy	77.90%	1
Creepy	73.00%	2
Scary	65.30%	3
Surprising	43.80%	4
Smart	33.00%	5
Relevant	32.40%	6
Evil	31.20%	7
Useful	24.30%	8
Good	10.50%	9

To get a better understanding of some of the activities that respondents participated in while online over the past twelve months, we provided a list of some of the more common activities such as making purchases, listening to music, watching videos and engaging in social media. Table B14 shows the full range of activities along with the percentage of “yes” and “no” responses; the top responses by percentage were watching videos (95.9%), using Google maps (93.1%) and making purchases (92.5%). There were three (Upload photos – 1; Online Banking – 1 and Twitter – 1) missing values in which we imputed with the mean for that activity. Surprisingly, only 33.9% have clicked on a pop-up ad, which is an online advertisement that appears over the browser window of a website that a person has visited (www.webopedia.com); perhaps this may be attributable to Online Information Privacy Concerns. While we did not specifically measure Internet activity engagement and its impact on perceived creepiness, in reviewing the overall results, it appears as if the level of engagement on the Internet does not necessarily change the degree to which something may be perceived as creepy.

Table B14. Activities Performed Online Within the Past 12 Months

Internet Activities (N=389)	Yes	No
Watched online videos	95.90%	4.10%
Used an online mapping service such as Google Maps or MapQuest	93.10%	6.90%
Purchased products and services online such as music, books or clothing	92.50%	7.50%
Participated in a social network such as Facebook, or a professional network such as LinkedIn	89.20%	10.80%
Read a newspaper or magazine online	88.70%	11.30%
Posted or read a blog or bulletin board on a website	86.40%	13.60%
Performed online banking or other money management activities such as buying stocks or bonds	86.00%	14.00%
Uploaded photos to a social network or other type of website	74.00%	26.00%
Used a membership to rent or stream movies or TV shows from Netflix or similar service	66.30%	33.70%
Downloaded music	65.80%	34.20%
Used Twitter	62.00%	38.00%
Sold or bought on eBay, Craig's list or similar site	61.20%	38.80%
Used Instagram	36.20%	63.80%
Clicked on a pop-up ad	33.90%	66.10%
Used SnapChat	15.90%	84.10%

Respondents were also asked if, over the past twelve months, they had participated or performed activities to safeguard their privacy or protect their personal information. Eighty-two percent of the respondents refused to give information to a website because they felt it was too personal or unnecessary, 78% have opted-out of receiving customized online advertisements, and 67% have decided not to use a website or make an online purchase because they were not sure how their personal information would be used. While this does not specifically speak to perceived creepiness, it does provide a lens to the concern some consumers have about the collection and use of their personal information while online. Also, this informs us that consumers will take measures to protect their personal information and privacy from nefarious uses, which could include “creepy” communications.

Table B15 shows some of the activities in which consumers engage to protect their personal information along with the percentage of “yes” and “no” responses.

Table B15. Internet Activities to Safeguard Privacy

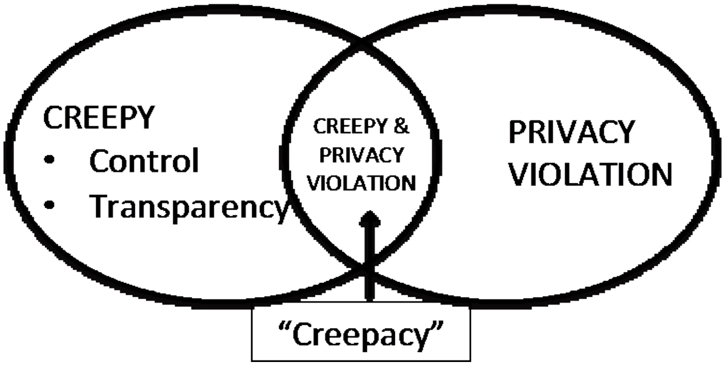
Internet Activities to Safeguard Privacy (N=389)	Yes	No
Refused to give information to a website because you felt it was too personal or unnecessary	82.00%	18.00%
Opted out of receiving customized online advertisements	78.00%	22.00%
Decided not to use a website or not purchase something online because you were not sure how your personal information would be used	67.00%	33.00%
Read a website's privacy policy	65.60%	34.40%
Provided false or fictitious information to a website when asked to register	63.00%	37.00%
Asked a website to remove your name and address from any lists used for marketing purposes	58.60%	41.40%
Created a fictitious email address to give to online companies	57.60%	42.40%
Set your browser to reject cookies	56.00%	44.00%
Asked a website not to share your name or other personal information with other companies	55.30%	44.70%

Discussion

In our quantitative study, we set out to determine the extent to which key factors that have been identified in prior studies relating to online information privacy as well as our qualitative study affect an unsolicited marketing advertisement, communication or tailored customer experience to be perceived as creepy. We know that feelings and perceptions of creepiness exist; however, less is known about what factors actually contribute to marketing communications to be perceived as creepy. Additionally, we wanted to examine the role of consumer-firm trust as a mediator between the endogenous and exogenous variables.

While extant literature is minimal on perceived creepiness, we looked to the literature and studies related to consumer privacy, specifically online information privacy as we have discovered in our prior study that creepiness and privacy are related but different. Not all personalized messages are creepy and not all personalized messages are privacy intrusive; thus, the premise is that creepiness and privacy are related but different. Figure B4 provides a visual representation of the relationship between personalized messages that are violations of privacy and those that are perceived to be creepy. However, because of the relatedness of these two factors, we anticipated that perceived creepiness and privacy to act in a similar fashion with and in relation to other variables.

Figure B4. Creepy & Privacy Violations



A consumer's digital footprint is at the center of our discussion on perceived creepiness because it is the consumer's data that is obtained or left behind creating a digital footprint and then aggregated to deliver personalized communications. According to (Madden, Fox, Smith, & Vitak, 2007), a digital footprint is comprised of an active and a passive digital footprint. The active footprint is the information that is knowingly provided such as name, address or email address when conducting a transaction; whereas, the passive footprint is the information that is collected about an individual without their knowledge, such as browsing activities when on the Internet.

Chellappa and Sin (2005) define personalization as "the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information" (p. 181); however, in order to be successful, personalization relies on the vendors' ability to acquire and process consumer information and also for the consumer to be willing to share information about themselves. Pertinent to both of these definitions is that the consumer willingly provides information about his/herself. However, the tension arises when information is collected and used in ways unbeknownst to the consumer. Our definition of creepy as "an emotional reaction to an unsolicited marketing communication, notification or interaction where personal information has been collected and unknowingly used, invoking feelings of apprehensiveness and disconcertment" captures the essence of the consumers' disadvantage of not knowing how their personal information is collected and used. The factors we identified to impact creepiness are online information privacy concerns, perceived anonymity, transparency and control, all of which are tied to the consumer having an awareness of what is going on and being in control over the collection and use of their data.

We found that the factors that we identified do impact the perceptions of creepiness. As we expected, Online Information Privacy concerns has a positive impact on perceived creepiness and the other factors: perceived anonymity, transparency and control negatively impact perceived creepiness. Much to our surprise, trust did not have a mediating effect between the factors and perceived creepiness.

Online Information Privacy Concerns

Online Information Privacy Concerns had a positive direct effect on perceived creepiness (.44, p=.001). The questions in this construct were centered on a consumer feeling worried about threats to information privacy and having a sensitivity to the way their personal information is handled. It stands to reason that if a consumer is concerned about their personal information, then any use of information for which they were not aware or expecting to be used for another purpose, then when it was initially provided, such as a personalized communication, would be perceived as creepy. Previous studies researching online privacy concerns (Culnan, 1993; Dinev et al., 2008; Dinev & Hart, 2006) show a relationship between a consumers' attitude about privacy and their willingness to disclose personal information. These findings corroborate our findings around online information privacy concerns in general.

Perceived Anonymity

When consumers are online, there is a perception of anonymity. Assuming anonymity to mean the inability to be identified (Merriam-Webster Online, 2012); while on the Internet, there is a sense that the activities performed online are confidential, private (Bates & Cox, 2008) and unknown in the virtual world. The Internet can provide a false sense of anonymity. In fact, the majority of individuals' activities and personal information is being monitored or tracked when online and consumers are aware of this fact because they often take steps to limit the amount of tracking such as clearing cookies and browser activities (Buchanan & Paine, 2007). Our study found that perceived anonymity had a negative effect (-.23, p=.001) on perceived creepiness. This was somewhat surprising in that we initially thought that if a consumer thought that they were anonymous, receiving a personalized communication would uncover the fact that they were not as anonymous as they originally believed and, therefore, perceptions of creepiness would increase.

Transparency

We associated transparency with having awareness or some type of notice or disclosure about how personal information would be collected, used and shared by online companies. Our studied showed that transparency had a negative effect (-0.11, p-value=.008) on perceived creepiness. This supported our hypothesis that transparency negatively affects transparency. As one is more aware of how their personal information is collected and used, they are not caught off guard or unsettled when their personal information is used to present to them a personalized communication or tailored customer experience. Although Awad and Krishan (2006) found that customers who require greater transparency over personal information are less willing to be profiled, in our study, it appears as if the unwillingness to be profiled does not seem to translate into the consumer having increased feelings of perceived creepiness.

Control

As expected, we found that control negatively (-.22, p=.001) impacts perceived creepiness. Control over how personal information is collected and used is prevalent in privacy literature. Most of the studies around control and privacy (Culnan, 1993; Goodwin, 1991; Laufer & Wolfe, 1977) seem to indicate that when a consumer has control over the collection and use of their personal information, they are less concerned about privacy violations; such is the case with perceived creepiness. When a consumer has control over how their personal information is collected, used and shared, they are inclined to be less “creeped out” by a personalized communication. One might even suggest that they would expect a personalized communication if they have willingly provided personal information. Since the consumer is in control over how their personal information is disseminated, they may as Chellappa and Sin (2005) suggest, be willing to give personal information in exchange for something of value that providing personalized information provides. Chellappa and Sin (2005) also state that the degree to which a consumer values personalization is two times more influential than their privacy concerns when determining whether to use personalized services.

Trust

Much has been studied in regard to trust and information privacy (Chellappa & Sin, 2005; Schoenbachler & Gordon, 2002) Dinev & Hart, 2002; McKnight, 1998). Most of which agree that a consumers' willingness to engage with an online company is based on a high degree of trust between the firm and the consumer (Schoenbachler & Gordon, 2002). In our study, we chose trust (consumer-firm) as mediating the relationships between online information privacy concerns, perceived anonymity, transparency, and control on perceived creepiness. The overall effect of trust as a mediator had a weak effect on perceived creepiness (-.08, p=.075). The initial premise for this was that the despite consumer online information privacy concerns, the consumers' perceived anonymity while online, the degree of transparency an online company has and the amount of control a consumer has over the collection and use of their data, trust would mediate those effects on perceived creepiness because if you felt that the online company was trustworthy, that would override any other factors that may lead to a consumers' perception of creepiness. However, this was not the case. After pondering this situation and trying to determine why the results were what they were, we concluded that perhaps one might be even more surprised by a company in whom you trusted, to collect and use your personal information in an unexpected way, thus invoking perceptions of creepiness. The relationship between Trust and the factors that we identified suggest that Trust may be better served as a moderator, dependent variable or even as an independent variable having a direct effect on perceived creepiness. The R-squared value for Trust as a mediator in our model was .55 compared to .54 with Trust removed from the model, thus confirming the slight mediating effect of Trust. One might suggest that regardless of the level of Trust that exists within a consumer-firm relationship, a personalized communication is perceived to be just as creepy as a personalized communication where consumer–firm trust was low or even non-existent.

Implications for Theory

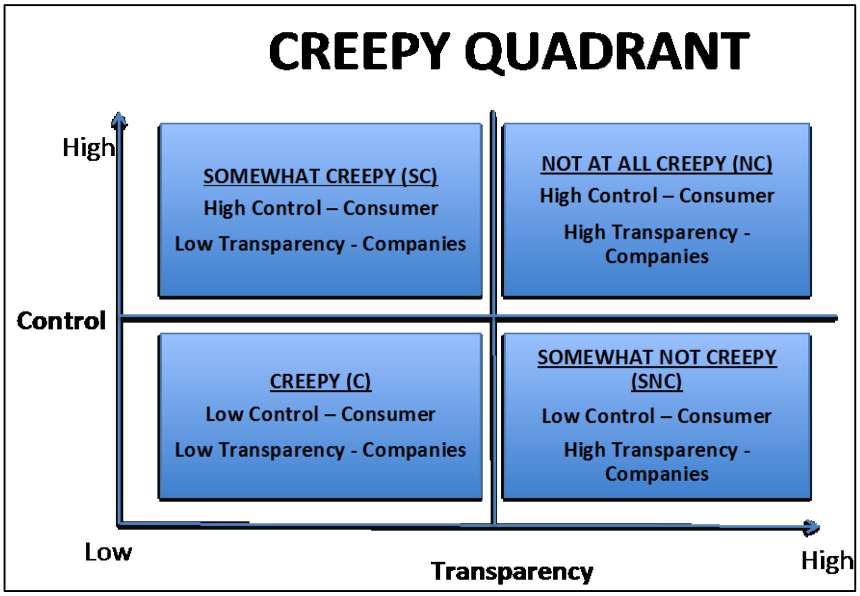
This study and the insights gained from this research contribute to the ongoing discussion regarding online privacy concerns, which is a key issue among consumers as evidenced by many studies, such as the Pew Research study (2014). This study also broaches the subject of privacy concerns expressed by consumers on the personalized marketing tactics of online companies in particular. Chellappa and Sin (2005) indicated very little academic research has been conducted on the value of personalized services: whether consumers need personalized services or whether they will use them given their privacy concerns.

Less has been studied on the feelings that unsolicited personalized communications generate when received by consumers. Not only does this research begin to fill a gap in the literature on the emotional response and cognitive aspects of privacy and targeted marketing what some have come to call “creepy”, but also it is prescient. Prescience is the “process of discerning or anticipating what we need to know and, equally important, of influencing the intellectual framing and dialogue about what we need to know” (Corley & Gioia, 2011: 13) While there may have been additional studies since Chellappa and Sin’s original study (2005) regarding personalized services and online behavioral marketing, the changes in technology and the ability to capture almost every activity of consumer activities online and offline, make researching personalized communication and experiences even more topical than it was ten years ago. According to Corley and Gioia (2011), prescient management theory can address such things as "social changes arising from technological advances, such as the value of privacy and artificial intelligence" (p. 24). Even though the study of creepiness seems to mimic privacy concerns or privacy violations, there is a difference between violations of privacy and perceived creepiness. Therefore, having an understanding of what is really behind "creepy" will be helpful in understanding specifically what actions should be taken to address and minimize consumers' concerns. Selinger (Selinger, 2012) suggests that identifying technologies as creepy is merely a crutch for getting to the root of what is behind those perceptions of creepiness. Although perceived creepiness and creepy marketing communications is discussed more so among practitioners than among academics, formulating a theoretical framework on perceived creepiness and where it fits within the privacy discourse can help guide practitioners, theorists, privacy advocates and regulators on the best approach for addressing a phenomenon that is relatively new but will continue to be an issue with the advent of advanced technology, the Internet of Things (IoT) and the amount of data being generated on a daily basis which is collected and used to create personalized marketing communications and tailored customer experiences.

Implications for Practice

This study highlights the key factors that are of concern to consumers: transparency and control over the collection and use of their personal information. Key findings from this research will enable companies to create marketing communications, interactions and a customer experience that addresses consumer attitudes toward these factors and mitigate any apprehensiveness or disconcertment a consumer may feel with online personalized communication. Our research confirms that if online companies are transparent with the consumers about their data collection, use and sharing activities, and provide them with some level of control over their data, customers may be less inclined to feel ambivalent about online personalized marketing communications. The Creepy Quadrant in Figure B5 shows possible relationships between control and transparency and its impact on the degree of perceived creepiness.

Figure B5. The Creepy Quadrant



Additionally, our study showed that consumer-firm trust does not mitigate the perception of creepiness; therefore, companies cannot just rely on the fact that they have a trusted brand or a trusting relationship with the consumer as a panacea for sending marketing communication that crosses the line from being cool to creepy. Additionally, knowing and understanding the key factors and the tipping point between cool and perceived creepiness will help to minimize consumers' privacy concerns for the way their data is collected, used and shared. Also, it can help marketers and online companies create campaigns and targeted ads that consumers perceive as relevant and useful as opposed to creepy or unsettling and have consumers wondering, “How did they get my personal information and know to send me that ad?” Further, data usage and privacy practices can be a differentiator and a competitive advantage; if companies do not implement good privacy practices and appropriately manage consumer data, sales and revenues can be affected directly and indirectly. Lastly, companies will have an increased awareness as to how personalized messages that are perceived as cool versus creepy can impact the companies’ brand, reputation, the level of trust a consumer has in a company, reputation, and overall customer experience.

Limitations

Perhaps the greatest limitation of this study is the subjectivity of the perception of creepy, thus the generalizability of our findings. What is creepy to one person may indeed be cool or relevant to another. Although the perception of creepy may vary from person to person, we hope that we have moved from the colloquium, “I know it when I see it,” popularized by Potter Stewart (1964) to identifying those key factors that are inherent in most communications that are perceived as creepy.

Another limitation may be the heavy concentration of MTurk respondents. Although it has been established that the data is diverse and of high quality, the issue still remains that some respondents may complete the survey just to obtain the compensation; albeit the compensation ranged from $1.35 to $1.50.

Lastly, but just as important is the environment of societal norms. Creepy is a word that is socially constructed and societal norms play an important role in determining what is indeed creepy. What is creepy at one point in time may be the norm in another point in time; therefore, determining what is creepy may be somewhat of a moving target, necessitating the need for a longitudinal study that re-evaluates and determines the context for which the communication was provided.

Future Research

While we identified key factors that may affect perceived creepiness, further examination of The Creepy Quadrant is worth examining utilizing real world examples of what many consumers have claimed to be creepy. This would enable us to ascertain if the relationship between transparency and control operate in the manner suggested in determining the degree of perceived creepiness of personalized communication. This research combined with the findings from our previous qualitative study on "creepy" pushes us to raise the question and make a call for Big Data ethics. With emerging technology that can watch, track and learn about us, there will be a need to provide boundaries that are aligned with conventional societal norms on what is the "right" use of this information. Although companies, marketers and other purveyors of data have the "right" (in that they are not doing anything illegal) to use the data that they collect, the question becomes "is what they are doing with the data the 'right' thing to do?" Scholars are just in the early stages of this conversation. As the Internet of Things (IoT) and "smart" technology becomes a reality and the norm, we will need direction on how best to provide consumers with the conveniences that they are seeking with "smart" devices without compromising privacy and coming across as creepy. The question becomes, "how can we continue to innovate without diminishing privacy and invoking the "creep factor?"

An offshoot of this is the idea of artificial intelligence. Some have stated that the rise of artificial intelligence in use today poses a threat to humans (Cellan-Jones, 2014). Will humans be needed if artificial intelligence is making many decisions for us based on data contained within our digital footprint? This is a question that we may have to reckon with in the very near future. Lohr (2015) poses the question, “If algorithms know all, how much should humans help?”[18]

Further exploration of companies’ being transparent and providing awareness and disclosing what they do with consumers’ personal data is warranted. Algorithmic transparency is another aspect of transparency worth researching. According to Ashkan Soltani, FTC’s Chief Technologist, consumers interact with algorithms on a daily basis, in most cases unknowingly. Soltani goes on further to say, “To date, we have very little insight as to how these algorithms operate, what incentives are behind them, what data is used and how it’s structured” (itworld.com, 2015).

Privacy by Design (PbD) is a framework that “is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures,” and one of its primary objectives is to ensure privacy and allow individuals to gain personal control over one’s information[19]. PbD is most often associated with the development of products and processes; therefore, researching and studying how PbD can be incorporated into smart devices and other technology that collects, uses, and shares personal information is an idea worth pursuing.

[18] http://www.nytimes.com/2015/04/07/upshot/if-algorithms-know-all-how-much-should-humans-help.html?_r=0

[19] www.ipc.on.ca/english/privacy/introduction-to-pbd

No doubt we are living in a data-driven society where almost every detail of our life is being captured, monitored, censored or surveyed upon; some have even said we are living in a surveillance society (Von Drehle, 2013) With rapid increases in technology and the amount of data being obtained on a daily basis, we will need to study and determine how we can coexist within this environment in a manner that is sustainable and without being privacy invasive and creepy.

Conclusion

The purpose of our research was to measure the degree to which key factors primarily online information privacy concerns, transparency, control, perceived anonymity and trust have on perceived creepiness in personalized marketing communications, advertisements and tailored customer experiences. With nearly 400 valid responses to our online survey, we have found that transparency, control and perceived anonymity negatively affect perceived creepiness and consumer–firm trust does not mediate these relationships.

Our study continues in the scholarly conversation of the impacts of Big Data on consumer privacy while also providing insight to marketers, data aggregators, and other online companies. Knowledge gained from this study will also inform marketers and online companies that they cannot solely rely on the trusting relationship that they have with the consumer to mitigate any perceptions of creepy. Instead, they must create personalized communications that walk the fine line of being relevant, innovative and customer-centric without being creepy, privacy invasive and creating feelings of disconcertment.

With continued advances in technology and more tracking and monitoring mechanisms in place to capture consumer behavior, oftentimes without their knowledge, it will be incumbent that those involved will self-regulate their actions and act in an ethical matter, as there are not currently any governmental regulations in place to guide this behavior. While creepy is a term that has been socially constructed to describe those personalized communications that invoke feelings of apprehension, it will be important for companies to not only be aware of the factors that can cause perceptions of creepiness but to move beyond creepy and get a better understanding of what is really behind the apprehension and disconcertment. This study is a foray into the broader discussion of the need for Big Data ethics in this Information Age, particularly transparency by companies on their data collection and use practices.

Appendix B1: Online Survey

Q1 For purposes of this survey, "Online companies" refers to any company that you interact with while online; "Personal Information" refers to any information about you.

Q2 Please rate the following statements regarding Trust of Online Companies

Generally, online companies use extensive security measures to safeguard consumers' personal information. (1)

Online companies are truthful when addressing consumer data collection and use policies. (2)

Generally, online companies are trustworthy in handling my personal information. (3)

I trust online companies to be honest with me when it comes to using my personal information. (4)

Online companies act in my best interests when dealing with my personal information. (5)

Q3 For purposes of this survey, Transparency refers to the degree online companies state how they are collecting, using and sharing your personal information.

Q4 Please rate the following statements regarding Transparency of Online Companies

I believe that online companies are transparent regarding the way they use my personal information. (1)

Online companies' consumer privacy notices about how my personal information is collected, processed, used and shared are clear. (2)

Consumer privacy notices for online companies are easily accessible. (3)

I believe that online company's consumer data collection and use policies are readily accessible. (4)

It is very important to me that I am aware and knowledgeable about how my personal information will be used by online companies. (5)

Online companies using my personal information are straightforward about the way they collect, process, use, and share my data. (6)

Q5 Please rate the following statements regarding your Perceptions of Surveillance and Anonymity while online

It bothers me that online companies may monitor my activities when I am browsing the Internet. (1)

It bothers me that online companies are following me on the Internet. (2)

I believe that as a result of my using the Internet, information about me that I consider private is being tracked by companies. (3)

When using the Internet, I believe my online location is monitored at least part of the time. (4)

Others cannot connect my identity to my online activity. (5)

It is easy for me to be anonymous when I am online. (6)

I feel confident that there is no way to specifically link my online activity to me. (7)

Online companies cannot identify me simply by my online behavior. (8)

If I don’t provide my personal information then I am anonymous to online companies. (9)

Q6 Please rate the following statements regarding the Collection and Use of Personal Information

It bothers me that social networking sites such as Facebook, LinkedIn and Twitter are collecting my personal information. (4)

It bothers me that online companies are collecting too much personal information about me. (6)

It bothers me to give personal information to online companies. (7)

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

It bothers me when online companies ask me for personal information. (3)

It bothers me that online companies share my personal information with other companies without my permission. (2)

When I give personal information to online companies, it worries me that those companies may use my information for other purposes. (1)

It bothers me that online companies may use my personal information for other purposes without my permission. (8)

Q7 Please rate the following statements regarding Online Privacy

I wish my personal information was not so easily accessible to online companies. (1)

Compared to other people I know, I tend to be more worried about threats to my information privacy. (2)

Compared to other people I know, I am more sensitive about the way online companies handle my personal information. (3)

Q8 Please rate the following statements regarding Control over personal information while online

I believe I have control over what personal information is shared by online companies. (1)

I believe I have control over how my personal information is used by online companies. (2)

I believe I can control who can access my personal information after it is collected by online companies. (3)

I believe I can control the personal information I provide to online companies. (4)

Q9 Please rate the following statements regarding personalized marketing communications or advertisements

I think personalized ads that collect and use my personal information without my knowledge are unsettling. (1)

I feel uneasy when I receive unsolicited personalized advertising from online companies. (2)

I feel threatened when online companies collect and use my personal information for unsolicited advertisements when I did not provide it for that purpose. (3)

I feel that as a result of my visiting websites, others who collect data about me have invaded my privacy. (4)

Personalized marketing communications are an invasion on my privacy. (5)

I feel that as a result of my using the Internet, information about me is out there and, if used, will invade my privacy. (6)

I am uncomfortable with amount of personal information online companies know about me as a result of my Internet use. (7)

I am worried about threats to my personal information. (8)

Q10 Unsolicited marketing communications and advertisements that use my personal information are:

Good (1)

Smart (2)

Useful (3)

Scary (4)

Creepy (5)

Relevant (6)

Surprising (7)

Evil (8)

Violation of my privacy (9)

Q11 The next set of questions are scenarios which were created for research purposes. Please follow the directions for each question and answer to the best of your ability.

Q12 Please carefully read and consider the following scenario before responding to the next two survey items. You search online for information about an upcoming vacation. You visit several travel sites to research airfares, airline schedules and hotels for different destinations, but do not book a hotel or a flight.

After browsing for vacation information, you visit a social networking site to catch up with your friends. While you are logged on, an ad appears from a travel agency that you were not familiar with for a vacation package for one of the destinations you had just researched. (1)

A couple of days later, you visit an online news site. While you are visiting the news site, an ad appears from the hotel where you are a member of their rewards program. The offer is for one of the destinations you had researched previously. (2)

Q13 Please carefully read and consider the following scenario before responding to the next two survey items. You are experiencing what you believe are flu-like symptoms. You search the Internet on a few health related sites for possible remedies.

Later in the day, you visit the site of an online retailer where you regularly shop to make a purchase. You notice ads appear for cold and flu medication. (1)

The next day while online, an ad appears from a local drugstore with a link to receive coupons for cold and flu medication. (2)

Q14 Please rate the extent to which the following situation is Creepy

One evening you are on your computer working on a report, when suddenly your computer crashes. The next morning you access your email and one of your messages is an offer for a discount on a new computer (same brand as the one that crashed). (1)

Q15 Please rate how TRUE or FALSE each statement is for you

I am always courteous even to people who are disagreeable. (1)

There have been occasions when I took advantage of someone. (2)

I sometimes try to get even rather than forgive and forget. (3)

I sometimes feel resentful when I don’t get my way. (4)

No matter who I’m talking to, I’m always a good listener. (5)

Q16 How long have you been using the Internet? (Number of Years)

Q17 Within the last 12 months, have you ever…? (Yes or No)

Purchased products and services online such as music, books or clothing (1)

Used a membership to rent or stream movies or TV shows from Netflix or similar service (2)

Posted or read a blog or bulletin board on a website (3)

Read a newspaper or magazine online (4)

Participated in a social network such as Facebook, or a professional network such as LinkedIn (5)

Watched online videos (6)

Uploaded photos to a social network or other type of website (7)

Performed online banking or other money management activities such as buying stocks or bonds (8)

Sold or bought on eBay, Craig's list or similar site (9)

Used an online mapping service such as Google Maps or Mapquest (10)

Clicked on a pop-up ad (11)

Downloaded music (12)

Used Twitter (13)

Used Instagram (14)

Used SnapChat (15)

Q18 How many years ago did you make your first online purchase? (Number of Years)

Q19 On average, how many online purchases do you make each month? (Number of Purchases)

Q20 Excluding email, how many hours a week do you spend online using a computer or mobile device to do things that are not work related?

Q21 Within the last 12 months, have you ever…?

Refused to give information to a website because you felt it was too personal or unnecessary (1)

Asked a website to remove your name and address from any lists used for marketing purposes (2)

Asked a website not to share your name or other personal information with other companies (3)

Decided not to use a website or not purchase something online because you were not sure how your personal information would be used (4)
Set your browser to reject cookies (5)
Provided false or fictitious information to a website when asked to register (6)
Created a fictitious email address to give to online companies (7)
Read a website's privacy policy (8)
Opted out of receiving customized online advertisements (9)

Q22 What is your age? (Years)
Q23 What is your gender? (Male or Female)
Q24 What is the highest educational level you have obtained?
Some high school; No Diploma (1)
High School Graduate (2)
Associates Degree (3)
Bachelor's Degree (4)
Master's Degree (5)
Professional Degree (6)
Doctorate Degree (7)

Appendix C: The Effect of Transparency, Control, and Trust on Perceived Creepiness of Online Personalized Communications (Study 3)

Abstract

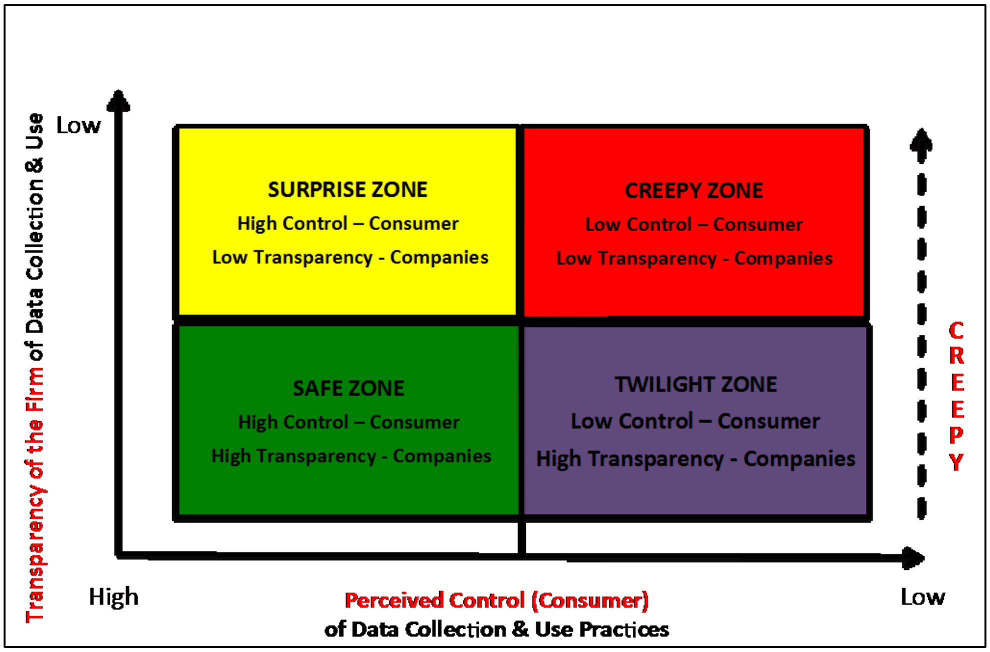
Perceived creepiness is an emotional response to an online experience, interaction, technology or unsolicited communication where personal information has been collected with one's knowledge and used in an unexpected or surprising manner invoking negative feelings. But what influences perceived creepiness? In this study, we examine the role transparency, control, context and trust play in users' perceptions of creepiness as it pertains to online personalized communications. A recent quantitative study confirmed that a firm's transparency about its data collection, use and sharing practices and providing the consumer control over the collection, use and sharing of his/her personal information can have a negative impact on perceived creepiness. But there is little understanding of how these factors interact and influence the overall experience. To this end, I conducted a set of experiments using a factorial 2x2 design involving control and transparency. I found that when a firm does not provide or disclose its data collection, use and sharing practices nor provides a mechanism for the consumer to control how their data is collected, used and shared and there is no way to manage this process, then perceptions of creepiness in personalized messages increases. I also found that the degree of trust a consumer has in the firm has a direct impact on perceived creepiness. High levels of trust reduce perceptions of creepiness and, conversely, low levels of trust increase perceptions of creepiness. I also confirmed that perceived creepiness has a negative impact on customer satisfaction, a key indicator of firm growth and competitive advantage. The findings suggest that marketers and online firms who take steps to be more transparent and provide the consumer with more control over their data, can reduce perceived creepiness and not diminish customer satisfaction which could otherwise harm brand reputation, sales, and revenue.

Keywords: Creepy marketing communications; personalized online advertisements; transparency; control; online privacy concerns; trust; behavioral marketing; data privacy; Big Data ethics.

Introduction

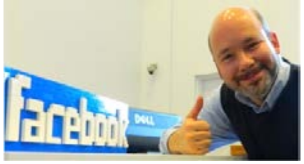
Smart, useful, scary, creepy (Ur et al., 2012). These are the perceptions of online behavioral advertising. Having a personalized communication such as an ad being smart, or useful or even scary is understandable, but what is creepy and what factors make a personalized message based in part on one's online message perceived as creepy? I define “creepy” as *an emotional reaction to an experience, interaction, technology or unsolicited communication where personal information has been collected with your knowledge and used in an unexpected or surprising manner invoking negative feelings.* In an earlier study (Stevens, 2014, 2015), that is a working paper in the Department of Design and Innovation at the Weatherhead School of Management, I identified and tested factors (perceived anonymity, perceived surveillance, online information privacy concerns, transparency, and control) that influence perceived creepiness. The data confirmed that transparency and control are key factors that lead to and have a negative impact on perceived creepiness. However, it is not just transparency by the firm of their data collection, use and sharing practices or control by the consumer over their personal information that contributes to a personalized message to be perceived as creepy. It is instead the interplay of these factors in real situations that influence perceived creepiness. The Creepy Quadrant (Figure C1) is a visual depiction of the potential interplay between transparency and control.

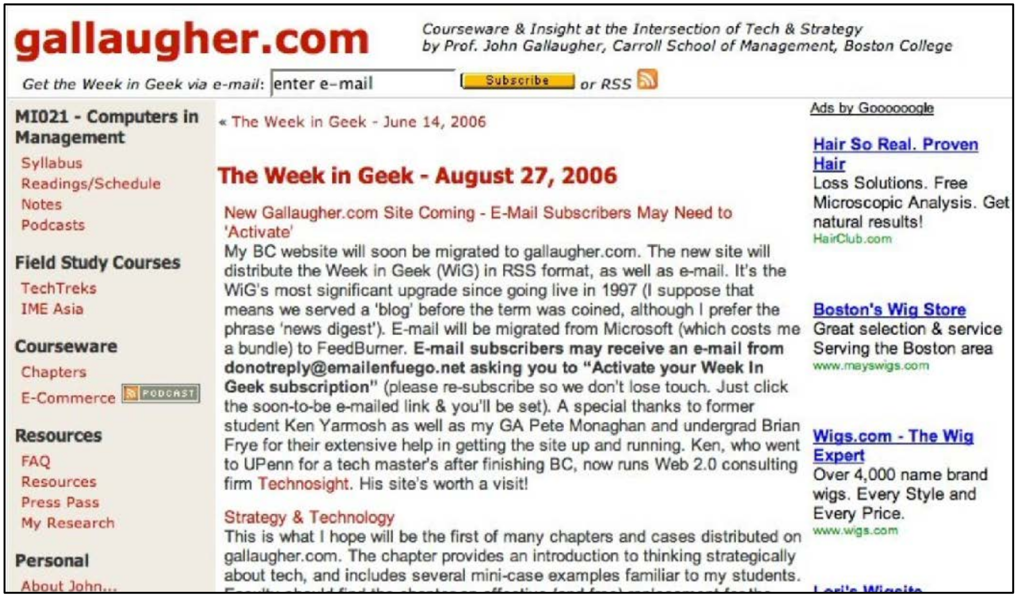
Figure C1. Creepy Quadrant


Transparency of the Firm of Data Collection & Use
Low
High
SURPRISE ZONE
High Control – Consumer
Low Transparency - Companies
CREEPY ZONE
Low Control – Consumer
Low Transparency - Companies
SAFE ZONE
High Control – Consumer
High Transparency - Companies
TWILIGHT ZONE
Low Control – Consumer
High Transparency - Companies
CREEPY
Perceived Control (Consumer)
of Data Collection & Use Practices
Low

Within the Creepy Quadrant, each of the four zones represents how the presence of, or lack of transparency and the presence of, or lack of control will impact a consumer’s perceptions of creepiness. The four zones are: creepy, safe, twilight and surprise. There are two extremes: creepy and safe; the other zones represent points along the creepy continuum. The “creepy” zone is characterized with no transparency by the firm and no control by the consumer. The “safe” zone is the area where the firm is transparent and the consumer has control. In this category, the personalized message is thought to be cool, smart and relevant. The next zone is the “twilight” zone. In this area, the firm is transparent, but the consumer has no control. Some may recall the Twilight Zone, a popular television show that appeared in the early 1960s, which showed, unrelated stories that were thrilling, suspenseful, horrific and usually ended with a surprising or unexpected ending. According to the dictionary (Merriam-Webster), the twilight zone refers to a conceptual area that is undefined or intermediate or an area that is confusing or unclear. This term seems to best identify this area within the Creepy Quadrant in that it is not definitively creepy or safe. In this zone, the consumer is aware that data is being collected, used and shared by the firm and also knows that the data will be used in a surprising way, but one has no way of controlling the situation. In the example in Figure C2, Week in Geek (WIG) is a newsletter affiliated with a consumer; however, key words and facts are being captured to deliver what is believed to be a relevant personalized message. However, despite how the consumer looks and the fact that the acronym for Week in Geek is WIG, the consumer is not interested in wigs, but in promoting his newsletter.

Figure C2. Week in Geek





gallaugher.com

Courseware & Insight at the Intersection of Tech & Strategy
by Prof. John Gallaugher, Carroll School of Management, Boston College

Get the Week in Geek via e-mail: enter e-mail *or RSS*

MI021 - Computers in Management
Syllabus
Readings/Schedule
Notes
Podcasts

Field Study Courses
TechTreks
IME Asia

Courseware
Chapters
E-Commerce

Resources
FAQ
Resources
Press Pass
My Research

Personal
About John...

« The Week in Geek - June 14, 2006

The Week in Geek - August 27, 2006

New Gallaugher.com Site Coming - E-Mail Subscribers May Need to 'Activate'

My BC website will soon be migrated to gallaugher.com. The new site will distribute the Week in Geek (WiG) in RSS format, as well as e-mail. It's the WiG's most significant upgrade since going live in 1997 (I suppose that means we served a 'blog' before the term was coined, although I prefer the phrase 'news digest'). E-mail will be migrated from Microsoft (which costs me a bundle) to FeedBurner. **E-mail subscribers may receive an e-mail from donotreply@emailenfuego.net asking you to "Activate your Week In Geek subscription"** (please re-subscribe so we don't lose touch. Just click the soon-to-be e-mailed link & you'll be set). A special thanks to former student Ken Yarmosh as well as my GA Pete Monaghan and undergrad Brian Frye for their extensive help in getting the site up and running. Ken, who went to UPenn for a tech master's after finishing BC, now runs Web 2.0 consulting firm Technosight. His site's worth a visit!

Strategy & Technology

This is what I hope will be the first of many chapters and cases distributed on gallaugher.com. The chapter provides an introduction to thinking strategically about tech, and includes several mini-case examples familiar to my students.

Ads by Goooooogle

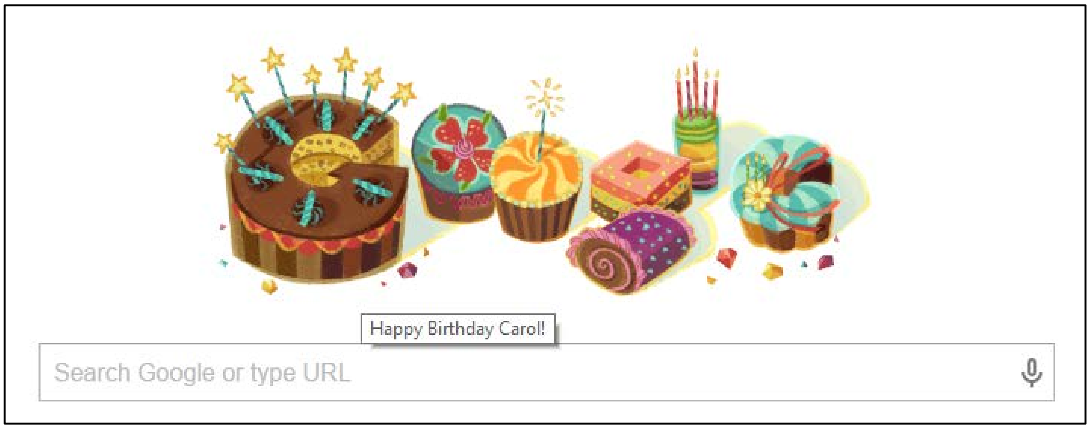
Hair So Real. Proven Hair
Loss Solutions. Free Microscopic Analysis. Get natural results!
HairClub.com

Boston's Wig Store
Great selection & service
Serving the Boston area
www.mayswigs.com

Wigs.com - The Wig Expert
Over 4,000 name brand wigs. Every Style and Every Price.
www.wigs.com

The last zone within the Creepy Quadrant is the “surprise” zone, in which the firm is not transparent, however, the consumer is in control. Although the consumer is in control, and can possibly control what information is collected or even opt-out, at some point, they are surprised about how their personal information that they willingly shared is used to generate a personalized communication. For example, Google uses one’s date of birth, which is required to sign up for an email account, to modify one’s Google doodle (Figure C3) on the given birth date.

Figure C3. Google Celebrates Your Birthday



The experimental study reported here is a confirmatory study to examine interactions between transparency and control and confirm earlier findings. One goal of the study is to re-validate the creepy scale/construct, but in this study we also extend our analysis to test the validity of the Creepy and Safe zones within the Creepy Quadrant by analyzing predictions based on the interaction of the two dimensions; transparency and control. By validating the Creepy Quadrant, we hope to be able to assess how the presence or lack of transparency and control contribute to a personalized message to become perceived as creepy. Ultimately, this will help to determine the extent to which transparency by the firm and the control allowed by the firm to consumers influence perceived creepiness of personalized marketing communications.

Although several studies recently have found that personalized messages (Ball, Coelho, & Vilares, 2006; Mittal & Lassar, 1996; Shankar, Smith, & Rangaswamy, 2003) as well as emotions (Mano & Oliver, 1993; Oliver, 1993) affect a consumers' level of satisfaction with a company, I want to also understand how creepy personalized messages impact the consumer's overall level of satisfaction with the company. One pivotal component to the level of customer satisfaction is the customer's trust in the company (Johnson & Auli, 1998). Accordingly, in this study, I want to assess whether consumer-firm trust impacts perceived creepiness of personalized communications. Additionally, I assess whether the context (content) of the message impacts the degree to which a message is perceived to be creepy. Nissenbaum (2004) speaks of contextual integrity and states that all areas of life are governed by informational norms: norms of appropriateness which refers to what information about an individual is appropriate to share within a particular context and norms of flow or distribution, which refers to the sharing of information with others. In my study, context pertains not only to the content of the message but also the norms. Nissenbaum (2004) suggest regarding information flows including how and from whom the message was received and the type of personal information that may have been used to create the message. This is important because the message may not be perceived to be creepy if the context in which it is used makes sense, or "in context." For example coupons from the grocery store based on items previously purchased may be fine as it is within the same context, however, a coupon for an item unrelated to your groceries, perhaps something that was searched for on the Internet would be “out of context”. In this study, we access context by testing three different email scenarios, which I suggest have varying degrees of perceived creepiness.

Overall, this study addresses the following research questions: 1) How do higher or lower levels of transparency and control impact perceived creepiness of personalized messages? 2) To what extent do creepy personalized messages impact the level of customer satisfaction with a firm? and 3) How does a consumers’ trust impact perceived creepiness? I conducted experiments using factorial 2x2 design with the help of survey vignettes (Jasso, 2006). Use of these techniques helps to tease out the impact of transparency and control and the degree to which a personalized marketing communication is perceived to be creepy

From an academic perspective, the findings will advance our understanding of perceived creepiness - a construct that has not been extensively studied but continues to be relevant as consumers express their concern over the collection and use of their personal information (Madden, 2014b; TRUSTe/National Cyber Security Alliance, 2016). From a practitioner perspective, the findings will inform marketers about the role of transparency and control as they create personalized marketing messages as well as how consumers feel when they perceive the company has not been transparent about its data collection and use practices. The findings from the study will also inform companies how consumers’ perceptions of creepiness of personalized message impact overall customer satisfaction of the firm, as well as provide marketers and online firms better understanding of why being a trustworthy company and engaging in trusting behaviors matter.

The remainder of the paper is organized as follows: First, I discuss the theoretical foundation on which my research is based. Next, I describe the research design and methods used in this study, followed by an analysis of the data and findings. Finally, I conclude with a discussion of the implications of the results for practitioners and researchers, as well as the study's limitations and suggestions for future research.

Theoretical Foundation Framework & Hypotheses Development

In this study, I examine two primary constructs: transparency and control, which have previously been identified as salient dimensions of perceived creepiness and form the basis of The Creepy Quadrant. Next, I test the extent to which context or contextual integrity (Nissenbaum, 2009) impacts whether a message is perceived to be creepy based on if it is regarded to be "within context" or "out of context" , I also explore how consumer firm trust impacts perceived creepiness, and finally, how perceived creepiness of personalized messages effects a consumers' overall satisfaction of the firm.

Transparency

In terms of perceived creepiness, transparency is key as I suggest that the presence or lack of transparency is central to what leads an online personalized communication to be perceived as creepy. If a firm has been transparent and disclosed what information it has collected about a person, how it is going to be used and with whom it will be shared, then receiving a message from one of the parties with whom the information was shared would make sense and the eeriness and mystery as to how that company got your information would be settled. In order to move beyond my tacit understanding of transparency and obtain a greater understanding of the depth and breadth of transparency, I surveyed the literature to see how transparency is defined and how it could be applied to perceived creepiness.

Transparency has varied meanings within different contexts. Often it is associated with compliance or even social responsibility. It has been widely studied across multiple disciplines with each providing a slightly different lens as to what transparency is and how it is operationalized. Schnackenberg and Tomlinson (2014) define transparency as the "perceived quality of intentionally shared information from a sender" (p. 5). Dapko (2012) and Eggert and Helm's (2003) definitions support the concept of being open and honest. Dapko defines transparency as "the extent to which a stakeholder perceives a firms' conduct is open and forthright regarding matters relevant to the stakeholder" (Dapko, 2012: 1). Eggert and Helm define transparency "as an individual's subjective perception of being informed about the relevant actions and properties of the other party in the interaction" (Eggert & Helm, 2003: 101). Although several authors (Schnackenberg & Tomlinson, 2014; Dapko, 2012; Eggert & Helm, 2003) have defined transparency, extant academic and practitioner literature does not provide a unified definition. Schnackenberg and Tomlinson (2014) suggest based on their literature review that transparency is a perception of received information. Further, they suggest that transparency is not a one-dimensional construct as others have suggested, but that it is multi-dimensional and consists of three specific dimensions: information disclosure, clarity and accuracy. When discussing Internet Users Privacy Information Concerns (IUPIC), transparency is accordingly referred to as awareness, which is having an understanding of data collection and use practices of an organization. Further, it refers to "the degree to which a consumer is concerned about his/her awareness of organizational information practices" (Culnan, 1995; Malhotra et al., 2004: 339) Foxman and Kilcoyne, 1993). Awareness under the IUPIC framework closely aligns with the disclosure dimension of the Schnackenberg and Tomlinson (2014) definition of transparency, however, it does not take into consideration the other dimensions transparency: clarity and accuracy. At the core of the myriad of definitions, transparency is about disclosing information in a manner that is perceived to be open and honest about the actions one takes and for the receiver of the information to have full access to the information that they want (Gebler, 2012). It has been stated, that "the advertising community has been woefully unforthcoming about how much data that they're collecting and what they're doing with it"[20]; perhaps implying a lack of transparency. Data brokers and data scientist are not exempt from being transparent. A report by the (Federal Trade Commission, 2014) issued a call for Data Brokers to be more transparent and held accountable for the data that they collect and it has been requested that data scientist be more transparent about algorithms that mine consumer information and enable the creation of personalized messages.[21]

Transparency is also the first principle of The Fair Information Practice Principles (FIPPs), a guiding framework to enhance consumer privacy while they conduct online transactions. FIPs states, organizations should be transparent and notify individuals regarding collection, use, dissemination and maintenance of personally identifiable information (PII) (Ware, 1973). Further, Schnackenberg and Tomlinson (2014) argue that disclosure is a key dimension of transparency and define it "as the perception that

[20] www.cmo.com/bigdataethics/4/3/2014

[21] http://www.ibmbigdatahub.com/blog/challenges-transparent-accountability-big-data-analytics, 2013; Parkkinen, 2015

relevant information is received in a timely manner" (p. 9). Transparency is operationalized through disclosure. (Kosack & Fung, 2014) looks at transparency from the perspective of corporate governance and states there are five pillars of transparency and disclosure, which include: truthfulness, completeness, materiality of information, timeliness and accessibility. These pillars align with the three dimensions of transparency (disclosure, clarity, and accuracy) as noted by Schnackenberg and Tomlinson (2014). Transparency and disclosure go hand in hand as they allow people to make informed decisions on whether to engage with a particular company. If a consumer is aware of not only the overall data usage policies of a company and the company has informed the consumer who is collecting the data, what information is being collected, how the information will be used and why, then the consumer's need for transparency may be met (Martin et al., 2014).

A viable means for most companies to be transparent and disclose its data use practice is the privacy notice, which explains to customers the companies' data use and privacy practices and includes what information the company collects, with whom it is shared and how the information is protected and safeguarded.[22]

Transparency is about being open and honest. To the extent that the firm is transparent to the consumer and discloses its data collection efforts, how they use and share consumer information at its disposal to create personalized messages, then perceptions of creepiness will be minimized. In my previous study, I validated that transparency negatively impacted perceived creepiness *(-0.11, p-value=.008),* which

[22] https://www.ftc.gov/tips-advice/business-center/guidance/brief-financial-privacy-requirements-gramm-leach-bliley-act (Retrieved 10/23/2015).

serves as our baseline. Therefore, in this study, we confirm the effect of transparency on perceived creepiness of personalized messages thus,

Hypothesis 1. Greater (Less) transparency by the firm will decrease (increase) perceived creepiness

Control

The other aspect of the Creepy Quadrant is *control*. Having personal control over how an individual's personal information is collected and used is a common theme in studies of personal data privacy. Having the ability to control what information is shared, with whom, and under what circumstances, is paramount in maintaining privacy and safeguarding one's personal information. As privacy is often defined in terms of control (Culnan, 1993; Westin, 1968). Sheehan and Hoy (2000) suggest that privacy concerns decrease as control over information (collection and use practices) increases. We apply this same assumption to perceived creepiness. As the level of control one has over personal information increases, the less a personalized communication is perceived to be creepy. Nowak and Phelps (Nowak & Phelps, 1992) suggest that consumers have little control over what happens after their data is collected and would welcome the opportunity to have more control over the collection and use of their personal information. However, when online, the consumer has minimal control over the collection and use of their data because of various tracking and monitoring tools that are in place to capture consumer behavior often without consumers' knowledge and the ability to opt out of such practices. Consumers who perceive that they have no control over their personal information in personalized messages are more inclined to feel vulnerable (Taylor et al., 2009) and we contend, more susceptible to perceptions of creepiness. As unintended uses of data are more prevalent when the consumer loses control over how their data is collected and used, perceptions of creepiness are also more likely to occur when personal information is unknowingly used to create personalized communications. Conversely, as consumers have control over the collection and use of their personal information that they have self-disclosed, they will be less inclined to be "creeped out" because they would know what personal information they have disclosed and, specifically what and how the information will be used and shared. As shown in the Creepy Quadrant (Figure C1), lack of transparency and lack of control when applied to personalized messages creates perceptions of creepiness (Creepy Zone).

Another aspect of the Creepy Quadrant and helping in our understanding of perceived creepiness is control. Control is having the ability to manage how one's personal information is collected, used and shared or having the ability to opt-out of a company's data collection, use or sharing methods. When the consumer loses control over how their data is collected and used, perceptions of creepiness are more likely to occur because personal information is unknowingly used to create personalized communications. However when the consumer has control over the collection and use of their personal information and or the ability to opt-out of receiving personalized communication, perceptions of creepiness are diminished. Again, in a previous study, I was able to validate that control does have a negative impact on perceived creepiness *(-0.22, p-value=.001),* which also serves as a baseline; therefore, this study confirms the impact of control on perceived creepiness, thus:

> *Hypothesis 2. Greater (less) Perceived Control by the consumer over the collection, use and sharing of their data will decrease (increase) perceived creepiness of personalized messages*

The Creepy Quadrant (Figure C1) is an interaction between transparency and control. In this study, we test two zones of the Creepy Quadrant: Creepy and Safe. While transparency and control independently negatively impact perceived creepiness, we suggest that the two taken together has an impact on perceived creepiness.

If a company is not transparent about their data collection, use, and sharing practices, and they do not allow the consumer to manage data collection, use and sharing practices, or provide a mechanism to opt-out, then

> *Hypothesis 3a. No transparency by the firm and no perceived control by the consumer will increase perceptions of creepiness (Creepy Zone).*

If a firm does disclose how they collect data, how it is used to create personalized messages and with whom they share data, then perceptions of creepiness are minimized because the consumer is aware of what is going on with their data and the surprise factor is lessened, then

> *Hypothesis 3b. Transparency by the firm and perceived control by the consumer will decrease perceptions of creepiness (Safe Zone)*

Consumer Firm Trust

There have been several studies on the role of trust in consumer –firm relationships on the Internet and within E-commerce (Garbarino & Johnson, 1999; Jøsang & Tran, 2000; Reichheld & Schefter, 2000; Urban, Sultan, & Qualls, 2000). Corbit, Thanasankit, and Yi (2003) suggest that trust is key in building relationships with consumers on the Internet. In this study, I explore the concept of consumer-firm trust. In particular, this study assesses whether trust has a moderating effect on perceived creepiness under different levels of control and transparency. For this study, I use the definition of trust espoused by Hosmer (1995): trust is one party's (*consumer/Internet*

User) optimistic expectation of the behavior of another (*firm*) when the party must make a decision about how to act under conditions of vulnerability and dependence. In particular, I want to determine what role trust plays in shaping perceptions of creepiness. By understanding the moderating effect of trust on perceived creepiness, we can ascertain whether trust in a firm can reduce the effects of personalized marketing communication that a consumer perceives to be creepy.

Online trust has been found to be a key driver of successful web business, and it impacts consumers' willingness to engage and transact online (Beldad et al., 2010; Urban et al., 2009). Marketing literature would suggest that trust plays a crucial role in the marketer-consumer relationship (Garbarino & Johnson, 1999; Moorman, Zaltman, & Deshpande, 1992). If a consumer trusts a company and believes that they will act in a trustworthy manner and not violate the Social Contract (Friend, 2004; Rawls, 1999), nor violate the Fair Information Practices Principles (Culnan & Armstrong, 1999) as it pertains to their personal data, it may be that a personalized communication may not be perceived to be creepy. Therefore, we posit that receiving a personalized marketing communication or ad from a trusted company would have an impact on the degree to which the communication is perceived to be creepy. Additionally, trust is noted as a key factor when marketing to consumers and using their personal information, to create personalized messages (Nowak & Phelps, 1992; Wang & Petrison, 1993). According to Morgan and Hunt (1994), trust is diminished if the consumer perceives that their personal information has been misused or used inappropriately; a personalized message that uses information in an unexpected way could be deemed as a misuse of information. Thus, *Hypotheses 4. Trust will positively moderate the effects of transparency on perceived creepiness, such that, a high (low) level of trust will decrease (increase) the effects of transparency on perceived creepiness.*

Hypotheses 5. Trust will positively moderate the effects of control on perceived creepiness, such that, a high (low) level of trust will decrease (increase) the effects of perceived control on perceived creepiness.

Customer Satisfaction

Customer satisfaction is a critical concept in marketing practice and business management. The customer satisfaction metrics help businesses manage and improve their business. Customer satisfaction is often thought to be an outcome of marketing activities and serves as a link between purchase, consumption and post-purchase feelings (Churchill, 1982). Given the impact of customer satisfaction on repeat sales and brand loyalty (Churchill, 1982), customer satisfaction/dissatisfaction (CS/D) has been extensively studied (Bearden & Teel, 1983; Bolton & Drew, 1991; Cadotte, Woodruff, & Jenkins, 1987; Oliver & DeSarbo, 1988; Oliver, 1983; Tse & Wilton, 1988; Westbrook, 1987). Much of the early literature focused on dissatisfaction and different attributes, which causes a consumer to be dissatisfied. However, later studies (Bolton & Drew, 1991; Oliver & DeSarbo, 1988; Tse & Wilton, 1988) have shown that understanding the determinants of customer satisfaction cannot be fully explained by the confirmation/disconfirmation framework. These studies showed that there are other factors that lead a consumer to be satisfied or dissatisfied with a product or service such as performance (Oliver & DeSarbo, 1988), an assimilation effect where the consumer bases his expectations and then satisfaction is compared to the level of expectation (Oliver, 1981) brand-based norms (Cadotte et al., 1987; Tse & Wilton, 1988), equity (Oliver & Swan, 1989) and attribution (Folkes, 1988). According to Oliver, "consumers are thought to be more satisfied when they perceive fair (i.e. equitable) treatment and when they attribute favorable outcomes to themselves and unfavorable ones to others" (Oliver, 1983: 419). Oliver and Westbrook (Westbrook & Oliver, 1991a; Westbrook, 1987) used Izard's Differential Emotions Scales (Izard, 1977) and concluded that consumers have two primary affect states: positive and negative. Positive affective states include joy and interest, whereas, negative affective states include anger, disgust, shame, guilt, fear, sadness and contempt (Bagozzi, Gopinath, & Nyer, 1999).

Studies related to the role of emotions in marketing found that satisfaction and consumption emotion may be related. Westbrook and Oliver (1991) define consumption emotion as "the set of emotional responses elicited specifically during product usage or consumption experiences, as described either by the distinctive categories of emotional experience and expression (joy, anger, and fear) or by the structural dimensions underlying emotional categories such as pleasantness/unpleasantness, relaxation/action or calmness or excitement" (Russell, 1979; Westbrook & Oliver, 1991a: 85). As I have defined perceived creepiness as an emotion, it is very possible that negative affect is triggered when a personalized communication that is perceived to be creepy is received, thus rendering the consumer to be overall dissatisfied with the company, so much so, that they do not consume the product or service because of their dissatisfaction with the companies data use practices not being transparent. Evaluating a company's Net Promoter Score[23], which is a customer satisfaction metric may help to confirm this conjecture.

[23] https://www.netpromoter.com/know/

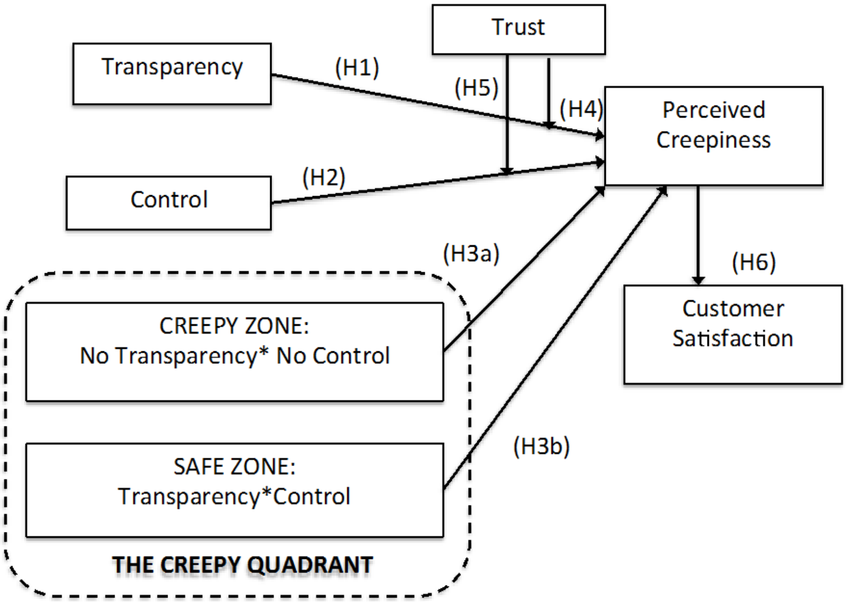
Customer Satisfaction is a key measurement that allows companies to gauge the degree of satisfaction of consuming their product or service. It can also be an indicator of loyalty, brand reputation and repeat purchases, which ultimately drives sales and revenue. Studies have shown that emotion, both positive and negative affect (Westbrook & Oliver, 1991b) can play a role in determining customer satisfaction. As perceived creepiness is an emotional (negative affect) response to a personalized communication, we posit that:

Hypotheses 6. Perceived Creepiness will have a negative effect on customer satisfaction.

Research Model

My research model is shown in Figure C4. The interaction (Transparency*Control) in our model represents the interplay of transparency and control; depicting the combination of the presence or absence of transparency, and control, which will help to validate the Creepy and Safe zones within the Creepy Quadrant (Figure C1).

Figure C4. Research Model



In this model, transparency represents the degree to which the firm is transparent about their data collection, use and sharing practices and control represents the ability of the consumer to opt-out or in some way control how their personal information is collected, used and or shared.

Research Design & Methods

To test and validate my research model, which shows the impacts of transparency and control on perceived creepiness, I used a 2x2 factorial design: Transparency vs. No Transparency and Control vs. No Control. Using factorial surveys vignettes makes it possible to create different treatment conditions and ascertain the relative weights of single variables that describe a situation (Auspurg et al., 2009; Jasso, 2006). Vignettes are short hypothetical stories in either written or pictorial form in which respondents can provide comments usually with survey type questions (Renold, 2002). Vignettes are most appropriate for capturing societal norms and attitudes about specific situation. Hughes states that vignettes are “stories about individuals, situations and structures which can make reference to important points in the study of perceptions, beliefs and attitudes (Hughes, 1998, P. 381). Furthermore, a factorial vignette methodology is used to identify normative judgments, which are dependent on contextual factors that the researcher can use to examine the influence of various elements of information used when the subjects make judgments. Additionally, through this method, researchers have the ability to better understand what the respondent is thinking and describe their judgments about complex constructs. Perceived creepiness is a complex construct due to its subjective nature and as previously noted because of the various factors that may influence perceived creepiness.

Given the complexity of perceived creepiness and that it is a judgment or belief that is in part based on societal norms the use factorial vignettes (Jasso, 2006) are justified. The factorial vignette method allows researchers to examine the effects of multiple factors simultaneously, such as with my study where I hypothesized the impact of several factors simultaneously on perceived creepiness: transparency, control, context, trust, and customer satisfaction.

The experiment was conducted in three stages; the first two stages were pre-tests, and the last stage was the actual experiment (Jasso, 2006). In stage one, I re-validated the Creepy scale that was created and used in a previous study to ensure its validity for the study. In stage two, I tested components of the hypothesized model and the treatment conditions associated with the Creepy Quadrant. Stage three was the final experiment which was carried out as a segmented survey across four treatment conditions (Wallander, 2009). The design combined the vignettes and constructs from the previous two pre-test, which were revised, based on the results and learnings from stage 2.

Vignette Development

I created vignettes to depict situations that could be perceived to be creepy. Based on the definition of creepy along with experiential information about personalized ads that were perceived to be creepy, I created scenarios that were expected to elicit a similar reaction. I created two pre-tests, one to measure transparency and control and the other to measure context being the content of the message in relation to the conditions or circumstances in which it was sent and contextual integrity which refers to the norms assocaited with information flow which includes transmission, communication, transfer, distribution, and dissemination (Nissenbaum, 2004). To test this, I created three different email scenarios that could be perceived to be creepy in varying degrees; and although I could have combined the transparency and control with the context and trust manipulations into one scenario, we chose to keep them separate in order to better understand the impact of the constructs on perceived creepiness. Following the vignette, the respondent answered survey questions adopted from established scales for transparency, data collection, use and sharing as well as for control and trust. Additionally, the perceived creepiness scale discussed in Appendix D was used along with three questions that were developed to measure transparency based on the three dimensions of transparency (disclosure, clarity, and accuracy) as defined by Schnackenberg and Tomlinson (2014).

Pre-Test Data Collection

We tested the scenarios using Amazon Mechanical Turk (MTurk).[24] For the study, the criteria were for respondents to be at least eighteen years of age and reside in the United States. The results from pre-tests 1 and 2 were analyzed and adjustments were made to the survey to address a few problem areas. Another pre-test was given to MTurkers and undergraduate college students at a university in the United States. For each test, the respondents were randomly allocated into different groups so that there would be an equal distribution among the various groups allowing me to test the differences of the statistical means between subjects.

[24] Amazon Mechanical Turk (MTurk) is an Internet crowdsourcing marketplace where requestors post jobs to complete, called a HIT (human intelligence task) and workers choose the HITs to complete for a small fee. Studies (Buhrmester, Kwang, & Samuel D. Gosling, 2011; Mason & Suri, 2012) have found that the reliability, quality and validity of the data generated MTurk respondents are just as valid and reliable as traditional research methods. MTurk users are heavily skewed towards respondents who use social media.

Pre-Tests Overview

When the Perceived Creepiness scale was developed, an extensive exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) were conducted during the pilot testing of the scale. All measures met acceptable thresholds for reliability and goodness of fit. Details of these results are in Appendix C3. Therefore, for this pre-test we did not perform additional EFA or CFA analysis. However, we did review the factor loadings, cross-loadings and communalities as appropriate to confirm that the data performed as expected. The data performed consistent with prior test and no issues or anomalies surfaced.

Stage 1 - Re-Validation of the Creepy Scale

To re-validate a subset (five items) of the perceived creepiness scale I used one factor, between subjects design. Subjects were provided one of two scenarios, one that was perceived to be creepy and one that was not. The purpose of this test was to confirm that the Creepy and Non-Creepy groups were significantly different. I recruited sixty-one respondents from Amazon Mechanical Turk. I did not obtain demographic information.

I performed a one-way ANOVA test that confirmed that our groups: Creepy and Non-Creepy were significantly different from each other. With this test, I was able to confirm that 1) Perceived creepiness can be measured (F=25.561, p=.000); Cronbach's Alpha for the five-item scale was .925 and 2) Perceived creepiness is distinct from non-creepy. The scenarios along with the test results are shown in Appendix C1.

Stage 2 - Vignette Manipulations –Transparency, Control, Context, and Trust

In stage two, I used factorial vignette surveys (Jasso, 2006) that varied transparency, control, and context. The constructs were separated into two separate experiments so that the effects of the constructs could be better understood. In pre-test 1, I measured transparency and control using existing scales to measure data use, data sharing and control along with the three questions that were developed based on the dimensions of transparency (Schnackenberg & Tomlinson, 2014). Eighty-nine subjects were recruited from Amazon Mechanical Turk. Demographic information was not collected. The pattern matrix showed strong loadings on separate factors; the three transparency factors of disclosure, clarity and accuracy loaded together along with Use, which leads me to believe that an aspect of Transparency is knowing how your personal information will be used. Cronbach's Alpha (.885) met the threshold showing acceptable reliability (Nunnally, 1978) of our constructs and the one-way ANOVA tests for Use (F=3.201, p=.000), Sharing (F=2.142, p=.01) and Transparency (F=3.179, p=.000) were found to be significant, confirming that a firm's transparency and having the ability to control the data collection, use and sharing does matter.

In pre-test 2, I measured context and trust. I obtained 85 responses from Amazon Mechanical Turk. These respondents were different from the first pre-test. Demographic data was not collected with this test. In this experiment, we provided two different scenarios and the respondents were randomized to only receive one of the two scenarios, which was followed by the Perceived Creepiness scale along with an existing scale to measure trust. The pattern matrix showed that all items from both constructs except Creep 4 and Trust 1 loaded cleanly onto separate factors. KMO was .873 and met acceptable thresholds (Hair et al., 2010), Bartlett's Test of Sphericity measured 772.154, df=45, p=.000. Cronbach's alphas for the two constructs improved when the problem items were removed as shown in table C1.

Table C1. Cronbach's Alpha for Creepy and Trust

Context/Trust		
Item	**Cronbach's Alpha – All Items**	**Cronbach's Alpha – After Items Removed**
Creep	0.742	.943
Trust	0.619	.948

Based on the results from the two pre-tests, several adjustments were made: 1) refined the Control scale to be more definitive; 2) tweaked the Share questions; and 3) Modified the Trust questions to be more specific to the hypothetical company used in the scenario. Next, a third pre-test was administered, where aspects from both pre-tests were combined; the provide/no provide condition with one of the scenarios was then followed by measures for testing perceived creepiness, trust, use, and control. The purpose of this test was to see how various components of the previous two pre-tests work together and confirm the reliability of the constructs and the manipulation check of the provide/not provide condition since the factors were isolated in the earlier tests. A total of ninety-six responses were obtained from Amazon Mechanical Turk and undergraduate students in a Marketing class from a college in the U.S. Again, no demographic data was collected. The final pre-test showed that two of the four constructs loaded together (Trust and Use). We did not remove the problem items (Creep4 and Trust1) that appeared in the second pre-test as we wanted to see how they would perform with the revised survey; the two items (Creep4 and Trust1) remained problematic. In looking at the Cronbach's Alphas with and without those items, the Cronbach Alpha improved from .730 to .783 when the items were removed. All of the constructs continued to show reliability. The vignettes along with key statistics from all three pre-tests are shown in Appendix C2.

Stage 3 – Final Experimental Survey

Based on the results from the pre-tests, revisions were made to refine the survey. The factorial vignette survey (Jasso, 2006) consisted of seventeen questions, pertaining to the constructs of perceived creepiness, transparency, control, trust and customer satisfaction along with demographic questions to capture age, gender and education level along with an attention checker to help determine whether the respondents were fully engaged with survey. In Table C2, I provide key information on the scales along with a couple of questions from each construct. Respondents were recruited from Amazon Mechanical Turk. Results and findings regarding the final experiment is detailed in the next sections.

Table C2. Overview of Scales

Construct	Number of Items	Scale	Source	Sample Questions	
Transparency	6	7-point Likert Scale - Strongly Agree - Strongly Disagree	IUPIC - Awareness of Privacy Practices Subscale - Transparency Malhotra, Kim and Agarwal, 2004; Used 2 of 5 items in scale - Consumer Perceptions of Transparency- Hustevdt and Kang 2013	I believe that online companies are transparent regarding the way they use my personal information	I believe that online company's consumer data collection and use policies are readily accessible
Control	4	7-point Likert Scale - Strongly Agree - Strongly Disagree	Privacy Control - Xu et al, 2011	I believe I have control over what personal information is shared by online companies.	I believe I can control who can access my personal information after it is collected by online companies.
Customer Satisfaction	**6**	7-point Likert Scale - Strongly Agree - Strongly Disagree; Facial - Happy to Sad	Churchill & Surprenant, 1982; Net Promoter Score	Overall, how satisfied are you with (Name of Company)	My experience with (Name of Company) was positive
Trust	**5**	7-point Likert Scale - Strongly Agree - Strongly Disagree	Jarvenpaa and Tractinsky, 1999 - 3 questions; Developing and Validating Trust Measures for E-Commerce, McKnight et al 2002	I trust that (Name of Company) keeps my best interest in mind when dealing with my personal information	(Name of Company) is honest with me when it comes to using my personal information
Perceived Creepiness	8	5-point Likert Scale - Anchored from "Not At All Creepy" to "Creepy"	4 questions - Privacy Intrusion - Xu et al., 2008; 4 self-developed	I feel uneasy when I receive unsolicited personalized advertising from online companies.	I feel threatened when online companies collect and use my personal information for unsolicited advertisements when I did not provide it for that purpose.

Sample & Data Collection

The survey was designed using Qualtrics software, where I was able to add randomization to the specific questions to ensure that assignment to the groups was random and equally distributed among the groups. Using Amazon Mechanical Turk, I collected 245 responses in December 2015. After removing incomplete and “faked” surveys, where the responses were either all “1s” or “7s”, there were 238 valid responses. Forty-six percent of the respondents were female, the average of the participants was thirty-five years old and 66% hold a college degree. The demographic breakdown of our sample is shown in Table C3.

Table C3. Demographics for Study 3

Item		Number	Percentage
Gender (N=238)	Male	129	54%
	Female	109	46%
	Not Reported	0	0%
Age (N=238)	18 - 27 (Millinieals)	62	26%
	28 - 43 (Gen X)	135	57%
	44 - 62 (Baby Boomer)	37	16%
	63+ (Traditionalist)	4	2%
	Not Reported	0	0%
Education Level (N=238)	Some high school; No Diploma	2	1%
	High School Graduate	78	33%
	Associates Degree	44	18%
	Bachelor's Degree	90	38%
	Master's Degree	22	9%
	Professional Degree	2	1%
	Doctorate Degree	0	0%
	Not Reported	0	0%

Measurement Model

To analyze the data (238 valid responses), adequacy and reliability measures were used to determine whether the results meet acceptable thresholds for various measures of adequacy and reliability. To glean meaningful insight from the data simple regression models were used for testing the data. Univariate analysis including ANOVA and

ANCOVA tests were also conducted, which are commonly used in behavioral research analysis.

Adequacy and Reliability Measures

To assess adequacy we reviewed the Kaiser-Meyer-Olkin (KMO) and Bartlett's Test for Sphericity. The Kaiser-Meyer-Olkin measure of sample adequacy was acceptable with a value of .948, (Hair et al., 2010) and Bartlett's test of Sphericity was significant (χ^2 = 6984.763, df 253, *p*= .000), indicating that the data was appropriate for our model (Hair et al., 2010).

Reliability was measured by Cronbach's Alpha for the six factors within our model to ensure that they met the recommended level of 0.70 (Nunnaly, 1978). Cronbach's Alpha for the overall model was .899. Table C4 shows the Cronbach's Alpha for the overall model as well as for each of the constructs.

Table C4. Cronbach's Alpha Measure of Reliability

Factor Label	Cronbach's Alpha	Number of Items
OVERALL MODEL	**0.899**	**22**
Perceived Creepiness	0.953	4
VF Satisfaction	0.951	4
VF Trust	0.952	4
Use	0.962	3
Transparency	0.941	3
Control	0.866	4

Manipulation Checks and Results

In our vignette, the respondent assumes that they are planning a vacation to celebrate their birthday in Rome, Italy with an online travel site. They provide the company, Vacation Finders with personal information such as contact information, date of birth, passport number as well as payment information. Our first experiment contained two conditions. In the first condition, Vacation Finders "provided" information explaining how they collect, use and share personal information along with a way in which for you (consumer) to control how Vacation Finders would share your personal information with other companies by providing an opt-out check out box; in our experiment, they did not check the box.

> *(Provide) Vacation Finders provided you with information explaining how they collect, use and share your personal information. Additionally, they provided you with a check box to opt-out out of them (Vacation Finders) sharing your personal information with other companies. You do not check the box.*

In the second condition, Vacation Finders "did not provide" information about their data collection, use and sharing practices, nor did they provide a way for you to control the information that they share with other companies.

> *(Did Not Provide) Vacation Finders did not provide you with information explaining how they collect, use and share your personal information. Additionally, they did not provide you with a way of opting out of them (Vacation Finders) sharing your personal information with other companies.*

First, respondents were randomly assigned through the Qualtrics software that was used to distribute the survey, either the "provide" or "did not provide" information group. The distribution of the groups is shown in Table C5.

Table C5. Provide/Not Provide Manipulation Groups

Group	Number (N=238)
VF_P (Provided information)	120
VF_NP (Did not provide information)	118

Following the manipulation of the two conditions, the participants responded to items measuring perceived creepiness, trust, use, transparency, and control.

The analysis showed that when a firm provides information about its data collection, use and sharing practices there is a significant difference as it pertains to control, use, transparency and control, compared to firms that do not disclose information about their data practices as shown in Table C6.

Table C6. Provide/No Provide Construct Summary

CONSTRUCT	0=PROVIDE, N=120; 1=NOT PROVIDE, N=118	MEAN	F-VALUE	SIGNIFICANCE LEVEL
TRUST	0	2.8875		
	1	4.3581		
			3.448	.000
USE	0	2.3278		
	1	4.5311		
			9.626	.000
TRANSPARENCY	0	2.7361		
	1	4.7232		
			8.773	.000
CONTROL	0	2.2875		
	1	3.8263		
			3.947	.000

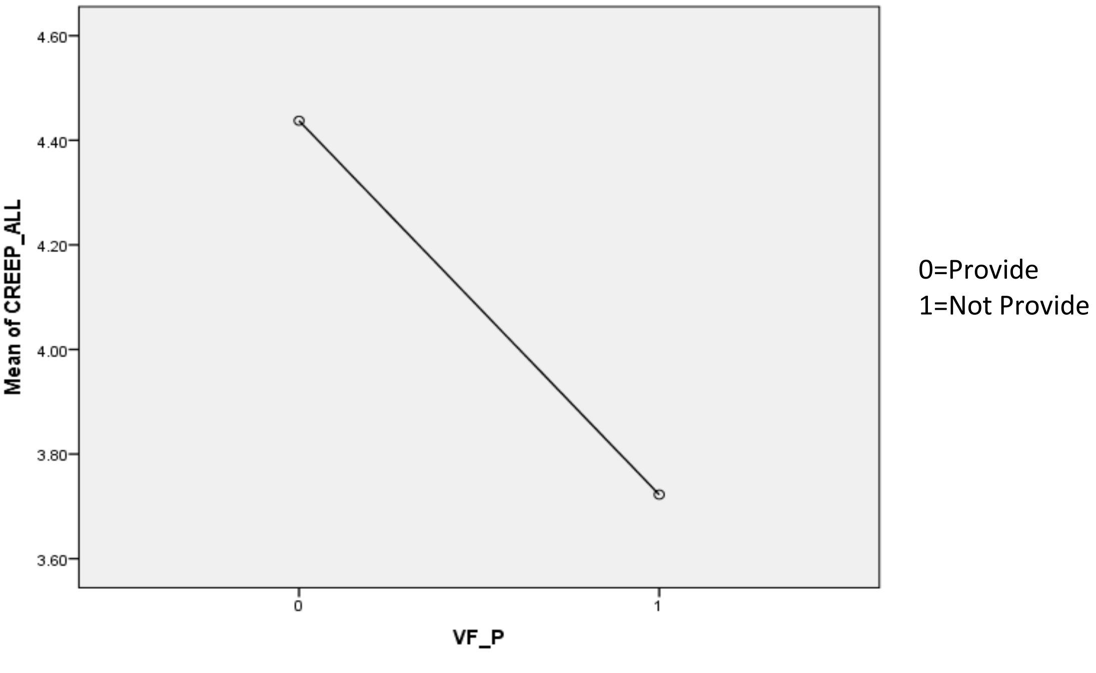
Conducting a one-way ANOVA test, I was able to determine that the manipulation checks for transparency and control were significant as evidenced in Table C7.

Table C7. One-way ANOVA Manipulation Check: Transparency & Control

Construct/Group		Sum of Squares	df	Mean Square	F	Significance
TRANS_ALL	Between Groups	234.912	1	234.912	122.521	‘0.000
	Within Groups	452.489	236	1.917		
	Total	687.401	237			
CONT_ALL	Between Groups	140.875	1	140.875	69.496	‘0.000
	Within Groups	478.395	236	2.027		
	Total	619.27	237			

Following this test, another test was conducted to determine if the provide/not provide condition effects perceived creepiness. There was a significant difference between the provide and not provide groups (Fvalue=10.380, p=.001) as shown in Figure C5. These results support Hypothesis 1, 2, 3a and 3b, in that when a company is transparent (provides) information about their data collection, use and sharing practices and gives consumers control over that information and the ability to opt-out, then perceptions of creepiness are decreased. For the experiment, I only tested the extremes of the Creepy Quadrant: Creepy Zone (“not provide” condition) and Safe Zone (“provide” condition) (Figure C1), as it was a challenge to tease out the other effects (Twilight Zone and Surprise Zone), which are points along the perceived creepiness continuum.

Figure C5. Provide/Not Provide Group Differences



The next experiment manipulated context in order to ascertain the impact on perceived creepiness.

Email

To test the effect of context on perceived creepiness, there were three email scenario contexts in which I was able to test the manipulations. The respondents were again randomized to receive one of three possible contextual email scenarios. One email was from a winery with whom Vacation Finders shared your personal information, offering wine tasting and winery tours only valid during the dates of your trip, herein referred to as wine;

> *Vacation Finders shares your information with a winery near Rome. After you book your trip, you receive an email from the winery providing information for wine tasting and winery tours that can only be used during the time of your trip.*

Another email was from a restaurant with which Vacation Finders also shared your personal, herein referred to as restaurant;

> *Vacation Finders shares your information with a restaurant close to where you live. After returning home from your vacation in Rome, Italy, you receive an email message from the restaurant; the subject line reads, "Welcome Home from Italy ~ Sorry We Missed Your Birthday." The email contains information about "birthday" dinner offers.*

In the last email, Vacation Finders shared information about your upcoming trip with your contacts, herein referred to as birthday.

> *Vacation Finders shares information about your upcoming trip with your contacts. They told your contacts to email the hotel where you will be staying while in Rome with "birthday greetings" for you. When you check into your hotel, you receive an email from the hotel; the subject line reads, "Your Friends Wish You a Happy Birthday". The email from the hotel contains the forwarded emails from your contacts, which are family members, close friends and business associates.*

Table C8 shows the distribution of the email group.

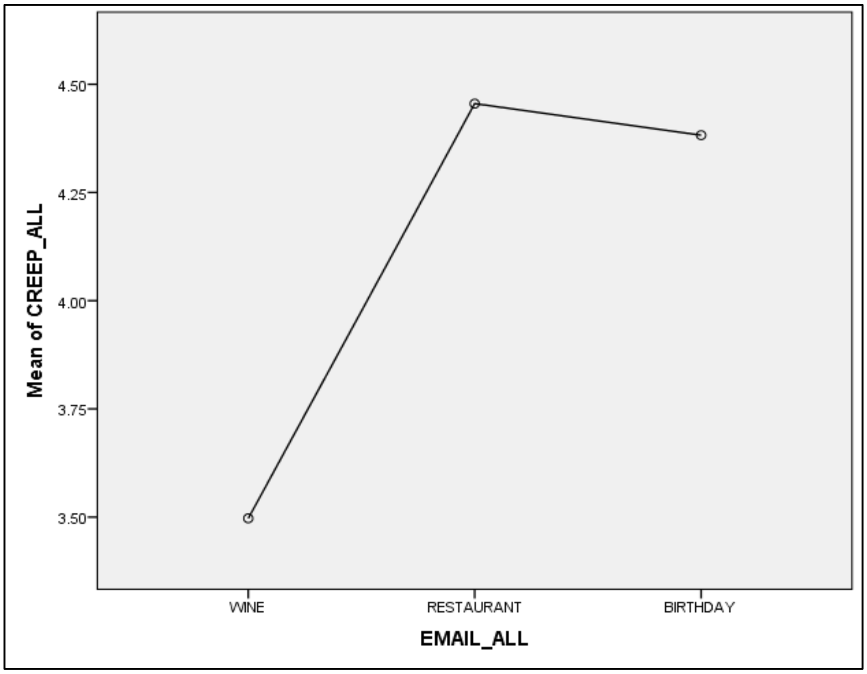
Table C8. Email Manipulation Groups

GROUP	NUMBER (N=238)
Wine	86
Restaurant	67
Birthday	85

Results

Given that perceived creepiness varies among the provide/not provide conditions, we tested whether perceived creepiness was significantly different among the three email scenario groups (context): wine, restaurant and birthday. We found that perceived creepiness does vary with context (email received) (F=8.073, p=.000). Figure C6 shows the difference between the three contextual email scenarios.

Figure C6. Contextual Scenario Differences



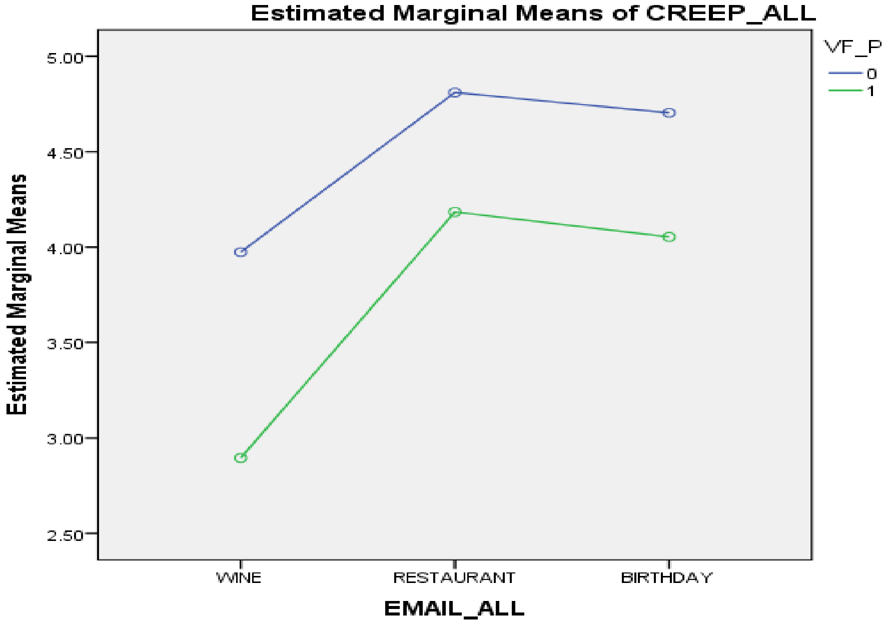
The means of the groups are shown in Table C9, indicating perceived creepiness for the restaurant group was stronger than the wine group and very close to the birthday group.

Table C9. Perceived Creepiness and Email Scenarios

EMAIL	NUMBER	MEAN
WINE	86	3.4971
RESTAURANT	67	4.4552
BIRTHDAY	85	4.3824
Total	238	4.083

The results from the manipulation checks were significant and showed that perceived creepiness does vary by context (email scenario), Next, I tested to see if the interaction between the two manipulations (provide/not provide and context) were significant. Although the email (Fvlaue=9.926, p=.000) and provide/not provide (Fvalue=13.064, p=.000) was significant, the interaction between the two was not significant (Fvalue=.480, p=.619), indicating that there is not a significant difference of perceived creepiness when information is not provided than when it is provided. However, context is slightly creepier when information is not provided than when it is provided. Figure C7 illustrates this point.

Figure C7. Interaction Provide/Not Provide & Email Scenario



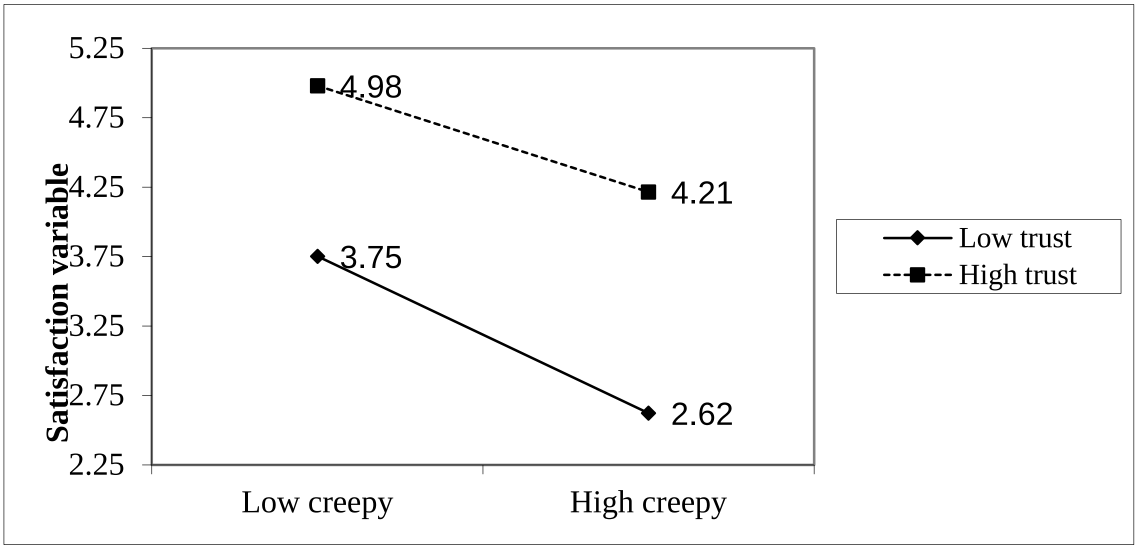
0=Provide
1=Not Provide

In this model, it was hypothesized that trust would have a moderating effect on perceived creepiness (H4 and H5). The results showed that trust had a direct impact (Fvalue=94.022, p=.000) on perceived creepiness. Another test was conducted to assess whether the provide/not provide condition had an impact on trust. The one-way ANOVA tests showed that the provide/not provide condition does impact trust (Fvalue=60.753, p=.000).

Several test were conducted based on a simple linear regression model since perceived creepiness and customer satisfaction are both continuous variables. Using a customer satisfaction scale (Churchill, 1982), the results from the regression model showed that trust also impacted customer satisfaction; as trust increases so does customer satisfaction (β=.429, p=.000).

Further, the relationship between trust and perceived creepiness and how it impacts customer satisfaction was tested. The relationship between trust and perceived creepiness was found to be significant (β=.032, p=<.05). In Figure C8, you will note that when trust is high, there is not much variation of when something is perceived to be highly creepy or mildly creepy, yet, when trust is low, there is a large drop in customer satisfaction when perceived creepiness is high versus when it is low.

Figure C8. Interaction between Perceived Creepiness and Customer Satisfaction



Another hypothesis was that Perceived Creepiness would have a negative effect on customer satisfaction (H6). In the model, it was supposed that perceived creepiness would impact customer satisfaction. The model was significant (F = 174.128 and p= 000), R2=.425 and β =-.485, p<.001, confirming that perceived creepiness has a negative impact on customer satisfaction To further test the concept of perceived creepiness and customer satisfaction, a much more complex model which also included the provide/not provide condition along with the three scenarios was also tested. I found that perceived creepiness was significant (β = -.466, p<.001); the provide/not provide condition was also significant (β=.294, p=<.05), however, the email scenario was not significant (β=-.016, p=.840).

In the survey, I also measured the effects of perceived creepiness on customer satisfaction by using the Net Promoter Score (NPS) (https://www.netpromoter.com/know), which is another metric, often used by businesses to measure customer's overall satisfaction with a product or service and customer loyalty (Reichheld, 2003). The NPS is also used as a predictor of growth; if a company's NPS is higher than their competitor it is stated that is very likely the company will outperform the market (https://www.netpromoter.com/know/). The NPS asks one question: "How likely is it that you would recommend [brand] to a friend or colleague?" and its rated on a 10-point scale with 1 being not likely and 10 being likely. The scores are categorized into three categories: 1) Detractors (0-6) – unhappy customers, 2) Passives (7-8) – satisfied but not enthusiastic, and 3) Promoters (9-10) – loyal enthusiasts. In my survey, the respondents were asked about their likeliness of recommending the fictitious company, Vacation Finders. The mean was 4.64 with a standard deviation of 2.82 indicating that the respondents fell into the Detractors (unhappy customers) category. Both of the tests regarding perceived creepiness and customer satisfaction support hypothesis six that states perceived creepiness will have a negative impact on customer satisfaction.

In this study, six hypotheses were tested, and all were supported. Table C10 displays the summary of the results of our hypothesis.

Table C10. Summary of Hypothesis

NUMBER	HYPOTHESIS	EVIDENCE	SUPPORTED
H1:	Transparency by the firm will have a negative effect on perceived creepiness	F=122.521, p=.000	Yes
H2:	Perceived Control by the consumer over the collection, use and sharing of their data will have a negative effect on perceived creepiness of personalized messages	F=69.496, p=.000	Yes
H3:	The Creepy Quadrant is an interplay between transparency and control such that:		
H3a:	No transparency by the firm and no perceived control by the consumer will increase perceptions of creepiness (Creepy Zone).	F=10.380, p=.001	Yes
H3b:	Transparency by the firm and perceived control by the consumer will decrease perceptions of creepiness (Safe Zone)	F=10.380, p=.001	Yes
H4:	Trust will positively moderate the effects of transparency on perceived creepiness, such that, a high (low) level of trust will decrease (increase) the effects of transparency on perceived creepiness	F=60.753, p=.000	Yes
H5:	Trust will positively moderate the effects of control on perceived creepiness, such that, a high (low) level of trust will decrease (increase) the effects of perceived control on perceived creepiness	F=60.753, p=.000	Yes
H6:	Perceived Creepiness will have a negative effect on customer satisfaction	β =-.485, p<.001	Yes

Discussion

In this study, I further confirmed that transparency and control are antecedents of perceived creepiness. Through the experiments, it was found that perceived creepiness decreases when the firm is more transparent about their data collection, use and sharing practices and provides consumers with some level of control as to how their data is collected used and shared. Marketers and online companies that are not transparent about their data collection and use practices create a problem that can ultimately affect customer satisfaction. Using the dimensions of transparency: disclosure, clarity and accuracy as described by Schnackenberg and Tomlinson (2014), for companies to be transparent, they must not only disclose their data use practices, but inform consumers what information that they have about them in a manner that is clear to the consumer as well as accurate. Combined with being transparent, the firm should also provide the consumer a control mechanism to 1) Correct or modify inaccurate information and 2) Opt-out of data collection, use and sharing practices for which they do not want to be a part.

Transparency is vital in maintaining a trusting relationship between the company and the consumer and it also provides a backdrop for the expectation of privacy when disclosing information. The study showed that when consumers trust the company, perceived creepiness decreases. This makes sense in that when a consumer trusts a company that they believe will act in their best interest as it pertains to collecting, using and sharing their data with 3rd parties, and when personalized online communication is received, perceptions of creepiness will be diminished. As trust is earned over time, it is in the companies' best interest to engage in trust-building behaviors, such as being transparent. Doing so not only impacts perceived creepiness but also builds trust.

Of particular interest to companies is customer satisfaction. Customer satisfaction can be a predictor of customer loyalty, brand image and overall company growth (Gustafsson, Johnson, & Roos, 2005). Although companies want to provide their customers with relevant communications, personalized communications that cross the line from being relevant to creepy do decrease customer satisfaction. Thus, it is important for companies to know whether the personalized messages that they are delivering are meeting expected outcomes and above all things not being perceived as creepy. Using the Net Promoter Score (NPS) along with the experiment results would further support the fact that perceived creepiness of personalized online communication has a definite impact on customer satisfaction.

In the experiments, only the extremes of the Creepy Quadrant: the Creepy and Safe Zones were tested and confirmed that when the company is not transparent and does not give the consumer some level of control over their data leads a personalized communication to be perceived as creepy. At the other extreme is the Safe Zone, where companies are transparent, and the consumer does have control over their data. Although transparency and control individually could impact perceived creepiness, the combination of the presence or lack of transparency and control provides a greater understanding of perceived creepiness as the two constructs together cover the consumer–firm relationship.

Post-Hoc Analysis

As there is not unified theory of creepy, I looked to other disciplines to help explain or understand perceived creepiness and the Creepy Quadrant—the interplay of transparency and control. One lens in which to view the Creepy Quadrant is Social Contract Theory. Social Contract Theory (SCT) (Rawls, 1999) is an implied agreement between an individual and the firm with whom they share their personal information. SCT posits that consumers and marketers enter into an implied social contract when they willingly exchange their personal information in exchange for something of value, such as access to a website or to obtain discounts (Dunfee et al., 1999; Friend, 2004). In fact, before disclosing personal information, consumers perform an analysis of the risk associated with disclosing personal information compared to the anticipated benefit; this is known as the Privacy Calculus (Laufer & Wolfe, 1977). When consumers share their personal information, they assume that the firm will take measures to collect, use and share a consumers' data in a responsible manner, if not, the Social Contract has been breached. Thus, a lack of transparency may be perceived as a breach of the Social Contract that is implicit between the firm and the consumer in addition to a violation of Fair Information Practice Principles (FIPPs).

Fair information practices (FIPS) (OECD, 1970) are a set of internationally recognized practices that addresses the privacy of information about individuals (Gellman, 2014) which "fairly balance the need for businesses to collect and use personal information with the legitimate privacy interests of consumers to be able to exercise control over the disclosure and subsequent uses of their personal information" (Milne & Culnan, 2002, p. 345). FIPs began in the 1970s with a report from the Department of Health, Education & Welfare, which have been revised several times over the years. In 2013, the Organization for Economic Cooperation and Development (OECD) revised the principles in a document that we are most familiar with today—FIPPS. Despite the changes to the principles over time, there are five core principles associated with FIPPS: transparency—ensures no secret data collection and provides information about the collection of personal data to allow users to make an informed choice; choice—gives individuals a choice as to how their information will be used; information review and correction—allows individuals the right to review and correct personal information; information protection—requires organizations to protect the quality and integrity of personal information and accountability—holds organizations accountable for complying with FIPPs (https://security.berkeley.edu/fipps).

Procedural fairness is the perception by a consumer that an interaction in which they were a part was conducted fairly (Lind & Tyler, 1988). Factors that contribute to procedural fairness include voice and control (Folger & Greenberg, 1985; Lind & Tyler, 1988). Procedural fairness is operationalized through Fair Information Practices and is key to better understanding perceived creepiness because if the consumer perceives that they are being treated fairly, then it may be possible that perceptions of creepiness are minimized. Procedural fairness can also be linked to customer satisfaction. Research on privacy and fairness by Culnan and Armstrong (1999), put forth prior research (Berry, 1995; Clemmer & Schneider, 1996; Schneider & Bowen, 1995) that links customer satisfaction to being treated fairly.

As transparency and control lead to perceived creepiness, lack of transparency by the firm can be interpreted as a violation of procedural fairness such that the consumer feels that they were treated unfairly in the interaction (product/service consumption) for which they were apart. Thus, it is highly likely that an interaction that was perceived as creepy would cause a consumer to be dissatisfied with the interaction with the online company.

Implications

Scholarly Implications

This study and the insights gained from this research contribute to the ongoing discussion regarding online privacy concerns and consumer reaction to online communications (Chellappa & Sin, 2005). As less has been studied on the feelings that personalized communications generate when received unsolicited by consumers, this research begins to fill the gap on how consumers “experience” personalized communications and online behavioral advertising, more specifically, the emotional response and cognitive aspects of privacy and targeted marketing what some have come to call “creepy” (Ur et al., 2012). Scholarly literature is rich with data about transparency, control and customer satisfaction; yet, our study provides another lens as to the importance of companies being transparent about their data, collection, use, and sharing practices. Since perceived creepiness has not been widely studied, our study confirms the role that transparency, control, and trust play in ascertaining whether a personalized message is perceived to be creepy. Selinger (2012) suggests that identifying technologies as creepy is merely a crutch for getting to the root of what is behind those perceptions of creepiness. This study attempts to get to the root of what is behind or underpinning perceived creepiness.

Practitioner Implications

This study confirmed that transparency and control are antecedents of perceived creepiness. Marketers and online firms armed with the knowledge and understanding of the antecedents of perceived creepiness will help them to addresses consumer feelings of perceived creepiness and also to create and deliver personalized online communications, interactions and customer experiences that do not cross the line from being cool, relevant and useful to creepy. My research confirms that if online companies take steps to be transparent about their data collection, use and sharing practices and provide consumers with the ability to control how their data is collected, used and shared will help to mitigate any apprehensiveness or eeriness a consumer may feel about personalized online communications. Moreover, the study showed that there is a relationship between perceived creepiness and customer satisfaction. Companies that are aware of the downstream impacts of perceived creepiness (decreasing trust, lower customer satisfaction, and damage to the brand) can engage in behaviors that do not invoke these feelings, but in behaviors that are positive and leave the consumer with the feeling that they have been treated fairly.

Even though the study of creepiness seems to mimic privacy concerns or privacy violations, there is a difference between violations of privacy and perceived creepiness. Having an understanding what is really behind "creepy" will be helpful in understanding specifically what actions should be taken to address and minimize consumers' concerns.

Limitations

Undoubtedly, there may be more factors that lead to personalized ads to be perceived as creepy; however, this study only focused on transparency and control, as such there could be other combinations of factors that could make up the creepy quadrant. Although the Creepy Quadrant has four zones combining the presence or lack of transparency and control, this study only tested the Creepy and Safe zones. As the other zones are points along a continuum, it was a challenge to tease apart the effects of transparency and control in those zones. To do so, would require additional experiments and testing to ensure that the effects were accurately measured and reflective of the zones as it pertains to the combination of transparency and control. Another key limitation is the demographic reach of our study. Our study only focused on U.S. Internet users. It is very likely that perceptions of creepiness could vary by geography and or culture, as it is a subjective judgment influenced in part by cultural norms and prevailing privacy laws. The subjectivity of perceived creepiness is perhaps another limitation. What is creepy to one person at one point in time may not hold true for another person. The subjectivity of perceived creepiness can make the generalizability of the findings somewhat challenging.

However, to mitigate this limitation, there was an attempt to get to the underpinnings of perceived creepiness, which I have found to be transparency and control.

Future Research

With emerging technology that can watch, track and learn about us, there will be a need to provide boundaries that are aligned with conventional societal norms on what is the “right” use of this information. More importantly, companies will need to be more transparent about their data collection, use and sharing practices, but also the algorithms and models that are used to categorize and profile individuals. Lohr (2015) poses the question, “If algorithms know all, how much should humans help?” Algorithmic transparency is another aspect of transparency worth researching. According to Ashkan Soltani, FTC’s Chief Technologist, consumers interact with algorithms on daily basis, in most cases unknowingly; Soltani goes on further to say, “To date, we have very little insight as to how these algorithms operate, what incentives are behind them, what data is used and how it’s structured” (itworld.com, 2015).

The transparency of data brokers and how they collect, use and share data is worth researching as well. Understanding transparency from these perspectives may also help in furthering our understanding of perceived creepiness.

Appendix C1

Creepy/Non-Creepy Validation

Creepy Scenario:
One evening, you are working on a report on your laptop made by eMaxx that you have owned for several years. Suddenly, the computer crashes. The manufacturer's <u>warranty agreement has expired, so you did not call the Help Desk for assistance.</u> The next morning you access your email and notice one of your messages is an offer addressed personally to you from eMaxx for a discount on a new computer. You notice <u>another message that is from a computer repair company also addressed personally to you which states "COMPUTER CRASHED? WE CAN HELP" offering a discount for computer repair services.</u>

Non-Creepy Scenario:
One evening, you are working on a report on your laptop made by eMaxx that you have owned for several years. Suddenly, the computer crashes. The <u>manufacturer's warranty agreement has not expired, so you called the Help Desk for assistance.</u> The next morning you access your email and notice one of your messages is an offer addressed personally to you from eMaxx for a discount on a new computer.

Please tell us how receiving the personalized offer from eMaxx makes you feel (7-point Likert Scale – SD to SA)

- *It was unsettling to receive the offer*
- *The offer made me feel uneasy*
- *I felt threatened by the offer*
- *The offer invaded my privacy*
- *I felt uncomfortable when I received the offer*

We performed a one-way ANOVA test that confirmed that our groups were significantly different. The test results are shown in table 2.

Table C1.1. Creepy One-way ANOVA & Reliability Results

CREEPY				
Item	**N**	**Mean**	**Significance**	**Threshold**
0 - Creepy	29	5.4552	0.000	> 5
1 - NonCreepy	32	3.4313	0.000	< 4
Total	**61**			
Cronbach Alpha = .925 for 5 items				

Appendix C2: Factorial Vignettes – Pre-test 1, 2 and 3

Pre-Test 1 - Transparency/Control

Situation: You are planning a vacation to celebrate a “Milestone Birthday”. You book a trip to Rome, Italy from an online travel site, Vacation Finders. In order to book your trip, you provide Vacation Finders with your contact information (name, address, phone number and email address) along with your date of birth, passport number and payment information (credit card number, expiration date and security code).

Manipulation (*Did Not Provide*) Vacation Finders did not provide you with information explaining how they collect, use and share your personal information. Additionally, they did not provide you with a way of opting out of them (Vacation Finders) sharing your personal information with other companies.

OR

Manipulation (*Provide*) Vacation Finders provided you with information explaining how they collect, use and share your personal information. Additionally, they provided you with a check box to opt-out out of them (Vacation Finders) sharing your personal information with other companies. You do not check the box.

Survey Scales

- Transparency: Disclosure, Clear, Accurate
- Data Collection
- Data Use
- Data Sharing
- Control

89 respondents

Results:

Table C2.1. Pattern Matrix – Pre-test 1

Pattern Matrix[a]

	Component		
	1	2	3
VF_USE1	0.941		
VF_USE2	0.933		
VF_USE3	0.983		
VF_CONT1			0.901
VF_CONT2			0.89
VF_CONT3			0.742
VF_CONT4			0.813
VF_SHARE1		0.87	
VF_SHARE2		0.888	
VF_SHARE3		0.903	
VF_SHARE4		0.875	
VF_DISC	0.923		
VF_CLEAR	0.971		
VF_ACCUR	0.824		

Extraction Method: Principal Component Analysis.
Rotation Method: Promax with Kaiser Normalization.
a. Rotation converged in 5 iterations.

Table C2.2. Cronbach's Alpha and KMO

Transparency/Control	
Item	**Cronbach's Alpha**
Data Use	0.962
Data Sharing	0.907
Control	0.859
Overall	0.838
KMO	0.795
Bartlett's Test of Sphericity	1149.451, df - 91, sig - .000

Pre-Test 2 - Context/Trust

Situation: You are planning a vacation to celebrate a “Milestone Birthday”. You book a trip to Rome, Italy from an online travel site, Vacation Finders. In order to book your trip, you provide Vacation Finders with your contact information (name, address, phone number and email address) along with your date of birth, passport number and payment information (credit card number, expiration date and security code).

Scenario *(Winery)* **-** Vacation Finders shares your information with a winery near Rome. After you book your trip, you receive an email from the winery providing information for wine tasting and winery tours that can only be used during the time of your trip.

OR

Scenario (*Restaurant*) Vacation Finders shares your information with a restaurant close to where you live. After returning home from your vacation in Rome, Italy, you receive an email message from the restaurant; the subject line reads, “Welcome Home from Italy ~ Sorry We Missed Your Birthday.” The email contains information about "birthday" dinner offers.

How much do you trust Vacation Finders?

______ I trust Vacation Finders

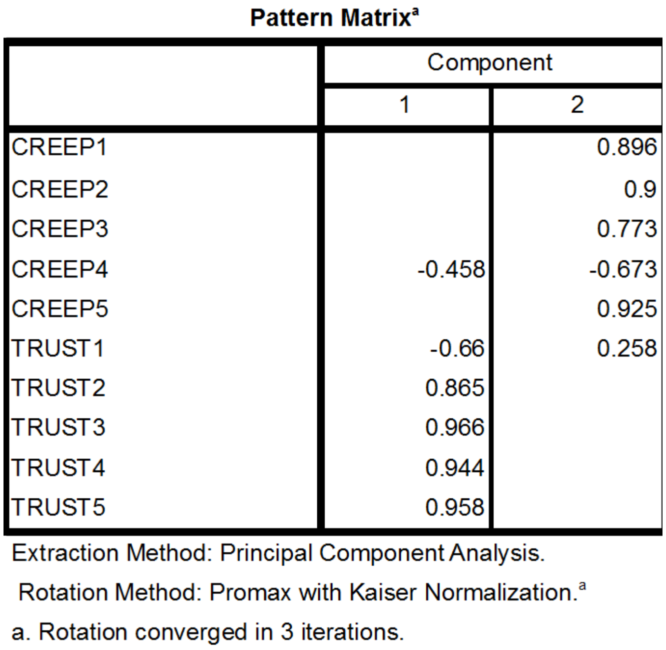
Survey Scales

- Creepy
- Trust

85 Respondents

Results:

Table C2.3. Pattern Matrix – Pre-test 2



Pattern Matrix[a]

	Component	
	1	2
CREEP1		0.896
CREEP2		0.9
CREEP3		0.773
CREEP4	-0.458	-0.673
CREEP5		0.925
TRUST1	-0.66	0.258
TRUST2	0.865	
TRUST3	0.966	
TRUST4	0.944	
TRUST5	0.958	

Extraction Method: Principal Component Analysis.
Rotation Method: Promax with Kaiser Normalization.[a]
a. Rotation converged in 3 iterations.

Table C2.4. Pattern Matrix – Pre-test 2

Context/Trust		
Item	**Cronbach's Alpha - All Items**	**Cronbach's Alpha - After Items Removed**
Creep4	0.742	0.943
Trust1	0.619	0.948
KMO	0.873	
Bartlett's Test of Sphericity	772.154, df - 45, sig - .000	

Pre-Test 3 – Combined

Situation: You are planning a vacation to celebrate a “Milestone Birthday”. You book a trip to Rome, Italy from an online travel site, Vacation Finders. In order to book your trip, you provide Vacation Finders with your contact information (name, address, phone number and email address) along with your date of birth, passport number and payment information (credit card number, expiration date and security code).

Manipulation *(Did Not Provide)* Vacation Finders did not provide you with information explaining how they collect, use and share your personal information. Additionally, they did not provide a way for you to control how they would share your personal information with the other companies.

OR

Manipulation *(Provide)* Vacation Finders provided you with information explaining how they collect, use and share your personal information. Additionally, as a way for you to control how they (Vacation Finders) share your personal information with other companies, they provided you with a check box to opt-out. However, you did not check the box.

Situation: Vacation Finders shares your personal information including your birthdate and vacation dates with a restaurant close to where you live. After returning home from your vacation in Rome, Italy, you receive an email message from the restaurant; the subject line reads, “Welcome Home from Italy ~ Sorry We Missed Your Birthday.” The email contains information about "birthday" dinner offers.

How much do you trust Vacation Finders? ______ I trust Vacation Finders

Survey Scales

- Creepy
- Trust
- Data Use
- Control

Results:

Table C2.5. Pattern Matrix – Pre-test 3

Pattern Matrix				
	Factor			
	1	2	3	4
CREEP1		0.881		
CREEP2		0.918		
CREEP3		0.742		-0.458
CREEP4		-0.496		
CREEP5		0.796		
TRUST1	-0.57	0.37		
TRUST2	0.853			
TRUST3	0.862			
TRUST4	0.928			
TRUST5	0.942			
USE1	0.786			
USE2	0.592		0.334	
USE3	0.8			
CONT1			0.966	
CONT2			0.978	
CONT3			0.893	
CONT4				0.815

Extraction Method: Principal Component Analysis.

Rotation Method: Promax with Kaiser Normalization.

Rotation converged in 6 iterations.

Table C2.6. Cronbach Alpha and KMO – Pre-test 3

Factor Label	Cronbach's Alpha	Number of Items
Overall Model - Initial	**0.73**	**17**
Revised (Removed Creep4 and Trust 1)	**0.783**	**15**
Perceived Creepiness	0.872	4
Trust	0.895	4
Use	0.93	3
Control	0.828	4

Appendix C3: Excerpt from Scale Development Process

To test the validity of the items in the perceived creepiness scale, I recruited participants from Amazon Mechanical Turk.[25] There were 131 completed surveys, however, after cleaning the data, 106 valid responses remained. Although the sample was small, it did meet the minimum sample size of 100 to 500 respondents for an initial exploratory factor analysis (EFA) (Mackenzie, Podsakoff, & Podsakoff, 2011). Performing an EFA is one means in which to measure and show evidence of construct validity, discriminant and convergent validity as well as internal consistency (Hinkin, 1998; T. R. Hinkin, 1995)

Using SPSS statistical software (V22 and V23), I was able to review the pattern matrix, communalities, scree plot and factor loadings; and also examine reliability, Kaiser-Meyer-Olkin (KMO) and Bartlett's Test of Sphericity. I used the Maximum Likelihood extraction method since we would be using the same extraction method within AMOS where I would be conducting confirmatory factor analysis (CFA), along with Promax rotation. Kaiser-Meyer-Olkin (KMO) measure of adequacy was .889 and Bartlett's Test of Sphericity was χ^2 = 2547.039, df 325, p= .000, both indicating the appropriateness of the data for factoring and the solution was not an identity matrix (Hair et al., 2010). Based on the Pattern Matrix, shown in table 1, the 8-item perceived creepiness scale showed convergent and discriminant validity as the eight "CREEP" items loaded strongly onto one factor; the other five constructs also loaded onto separate factors as well. One item (TRANS4) did cross-load with the Trust construct. It loaded on

[25] Amazon Mechanical Turk (MTurk), is an Internet crowdsourcing marketplace where requestors post jobs to complete, called a HIT (human intelligence task) and workers choose the HITs to complete for a small fee

the Trust construct at .322 and on the Transparency construct at .495. Based on this result, I did review the statements to determine if there was any ambiguity in the statements. I decided not to remove this item as it would cause me to omit this construct. Because of the strong loadings of the other items combined with the fact that transparency appeared in the qualitative study as a dominant theme of perceived creepiness, this item will be monitored when the scale is retested with a larger sample to see how it performs. Should it remain problematic, it will be removed.

Table C3.1. Pattern Matrix for 8-item Scale

Factor	**CREEP**	**PERCEIVED ANONYMITY**	**TRUST**	**CONTROL**	**ONLINE INFORMATION PRIVACY CONCERNS**	**TRANSPARENCY**
CONT1				**0.933**		
CONT2				**0.882**		
CONT3				**0.832**		
CONT4				**0.753**		
CREEP1	**0.714**					
CREEP2	**0.787**					
CREEP3	**0.883**					
CREEP4	**0.775**					
CREEP5	**0.749**					
CREEP6	**0.903**					
CREEP7	**0.860**					
CREEP8	**0.793**					
PA1		**0.841**				
PA2		**0.769**				
PA3		**0.952**				
PA4		**0.781**				
PA5		**0.710**				
TRANS3						**0.967**
TRANS4			0.322			**0.495**
TRUST1			**0.739**			
TRUST2			**0.798**			
TRUST3			**0.754**			
TRUST4			**0.800**			
TRUST5			**0.665**			
GEN2					**0.934**	
GEN3					**0.777**	
Extraction Method: Maximum Likelihood.						
Rotation Method: Promax with Kaiser Normalization.a						
a Rotation converged in 7 iterations.						

I also assessed reliability for each of the constructs and all exceeded the threshold of .70 (Nunnally, 1978). Cronbach's Alpha for the constructs are listed in Table C3.3; of most importance is the reliability measure for perceived creepiness, which was .942 for the eight items.

Table C3.2. Reliability Measures for Constructs

Factor Label	Cronbach's Alpha	Number of Items
Overall Model	**0.903**	**26**
Trust	0.925	5
Perceived Anonymity	0.929	5
Control	0.930	4
Online Information Privacy Concerns	0.923	2
Transparency	0.880	2
Perceived Creepiness	0.942	8

Fornell and Larcker (1981) suggest that examining composite reliability can also assess construct reliability. For the constructs, each of the composite reliability measures exceeded .70. I also examined Measures of Sampling Adequacy (MSA) across the diagonal of the anti-image matrix to ensure that they were above .70 (Dziuban & Shirkey, 1974), of which they were; values ranged from .842 to .940.

We conducted a confirmatory factory analysis (CFA), using AMOS software with Maximum Likelihood estimation to validate the established factor structure. We examined several fit statistics, including chi-square, CFI and RMSEA to ascertain the goodness of fit of the model and to determine if they met acceptable thresholds for an adequate fitting model (Hu & Bentler, 1995; Tabachnick & Fidell, 2007). Table C3.3 shows the estimates along with the significance levels of each of the items in the perceived creepiness scale.

Table C3.3. Perceived Creepiness Item Estimates

Item	Final	Estimates (Standardized)	Significance
CREEP1	I think personalized ads that collect and use my personal information without my knowledge are unsettling.	0.693	0.001
CREEP2	I feel uneasy when I receive unsolicited personalized advertising from online companies.	0.776	0.001
CREEP3	I feel threatened when online companies collect and use my personal information for unsolicited advertisements when I did not provide it for that purpose.	0.908	0.001
CREEP4	I feel that as a result of my visiting websites, others who collect data about me have invaded my privacy.	0.846	0.001
CREEP5	Personalized marketing communications are an invasion on my privacy.	0.797	0.001
CREEP6	I feel that as a result of my using the Internet, information about me is out there and, if used, will invade my privacy	0.851	0.001
CREEP7	I am uncomfortable with amount of personal information online companies know about me as a result of my Internet use.	0.843	0.001
CREEP8	I am worried about threats to my personal information	0.835	0.001

I also assessed construct validity by examining measures for convergent and discriminant validity. The construct met acceptable thresholds for convergent and discriminant validity as the composite ratio for all constructs exceeded .70 and AVE was greater than .50 (Fornell & Larcker, 1981), thereby, demonstrating construct validity as reflected in Table C3.4.

Table C3.4. Construct Validity Measures (N=106)

	CR (>0.70)	AVE (>0.50)	MSV	ASV
PRIV	0.923	0.858	0.386	0.088
CREEP	0.943	0.674	0.386	0.095
ANONYMITY	0.929	0.725	0.637	0.329
TRUST	0.927	0.719	0.637	0.367
CONTROL	0.931	0.773	0.523	0.265
TRANSP	0.883	0.790	0.627	0.300

Table C3.5 show the results of the goodness of fit measures based on the pattern matrix, from which we can conclude that the goodness of fit for the measurement model is sufficient as most of the values are within an acceptable ranges of the stated thresholds (Hu & Bentler, 1995; Tabachnick & Fidell, 2007: 715). Since the sample size is small, it is expected that some of the Goodness of Fit statistics will be impacted. Because of this, we left the model as is to test with a larger sample.

Table C3.5. Goodness of Fit Statistics

Goodness of fit statistics	Observed Value	Recommended
Statistical		
Chi-square	408.717	
Degrees of freedom (DF)	284	
CMIN/DF	1.44	Between 1 and 3
p-value	0.000	
Relative		
CFI	0.95	>0.950
TLI	0.942	>0.950
Absolute		
SRMR	0.046	<0.05
RMSEA (90% CI)	0.065	<0.060
RMSEA (Low/High)	.050/.078	
P-Close	0.05	>0.050
AGFI	0.735	>0.90

Appendix D: Development of Perceived Creepiness Scale

In my research, I purposefully identified characteristics of perceived creepiness as a new dimensional construct. After reviewing the limited literature related specifically to perceived creepiness, I could not identify a scale to measure it. Since there was no defined and validated scale for measuring perceived creepiness; I developed a scale to measure the negative affect of perceived creepiness. One of the articles on creepiness (Moore et al., 2015) suggested that an area for future research would be a development of scale to measure creepiness, hopefully, this scale will be a contribution to scholarship as well as to help practitioners assess the impact of perceived creepiness in the personalized messages that they create.

To guide my development of the scale, I referenced Churchill (1979), Hinkin (1998; 1995) and a recent rigorous method suggested by Mackenzie et al. for creating and validating a scale (Mackenzie et al., 2011). I mainly adopted the process for developing constructs and scales by Mackenzie et al. (2011) as it best reflects current understanding and expectations in developing scales. It is more extensive and recognizes especially conceptual sampling issues and the use of reflective and formative scales. The process of scale development as defined by Mackenzie et al. (2011) comprises ten specific activities, which fall into the categories of 1) Conceptualization, 2) Development of Measures, 3) Model Specification, 4) Scale Evaluation and Refinement, 5) Validation, and 6) Norm Development.

I will discuss the scale development process I followed to create the Perceived Creepiness Scale.

1. Conceptualization

According to Mackenzie et al. (2011), in the conceptualization stage, the conceptual domain of the construct is defined as well as what the construct represents. To conceptualize the construct, there are several steps that should be taken: 1) examine how the construct has been used in prior research; 2) specify the conceptual domain; 3) specify the theme of the construct; and 4) provide a definition that is precise. I will next discuss how I conceptualized the perceived creepiness scale taking these steps into consideration.

Prior research is limited as it pertains to perceived creepiness. In my literature review of perceived creepiness, I identified four studies that researched perceived creepiness within the context of personalized communications or online behavioral advertising, but none prescribed a scale in which to measure perceived creepiness.

In the first study, “Smart, Useful, Scary, Creepy” (Ur et al., 2012), the users expressed concern about the collection of their personal data as the basis for online behavioral advertising (OBA). Although the study mentioned creepy as a feeling respondents have about OBA, this study did not define creepiness or the factors that may lead to perceived creepiness, as that was not the focus of that research study; their perspective was describing the reaction to OBA.

Another study of creepiness was conducted by Tene and Polontesky (2013) in 2013, where they put forth: “A Theory of Creepy: Technology, Privacy and Shifting Social Norms.” The authors introduce the notion of creepy and provide the conditions where consumers are most like to experience creepy, which included unexpected data use or customization and the conditions in which perceived creepiness is apparent. It also discusses the subjectivity of creepy and the role of society and social norms in establishing what is perceived to be cool and acceptable versus what is perceived to be creepy. Although the article clarifies the conditions in which creepiness emerges, it did not define creepy nor identify specific factors that constitute perceived creepiness.

Barnard (2014) explore creepiness and its effect on consumer purchase intention in the study, "The Cost of Creepiness: How Online Behavioral Advertising Affects Consumer Purchase Intention." The creepiness factor is defined as "the sense that marketers are watching, tracking, following, assessing, and capitalizing on an individual's personal information or online activities that she perceived as private" (p. 6). Although Barnard (2014: 41) suggests under what conditions creepiness emerges, creepiness remains poorly defined, and the factors that make up perceived creepiness are not identified; neither is a scale to measure creepiness.

"Creepy Marketing: Three Dimensions of Perceived Excessive Online Privacy Violation" (Moore et al., 2015) is an explorative study, where the authors create a new construct, Creepy Marketing (CM). They discuss the impacts of personalized marketing on consumers and then make a differentiation between annoying marketing, which they define as tactics, and CM, which they define as feelings. Their approach to CM is from the perspective of personal space and virtual space. For this study, survey responses were categorized into four categories for which they also use to define CM: 1) Invasive tactics, 2) Causing consumer discomfort, 3) Violates social norms, and 4) Out of the ordinary tactics. It is from the first three categories that they develop the three dimensions of creepy marketing. Although the authors reference dimensions of CM, they do not explicitly indicate that these are dimensions that constitute creepiness or define what its antecedents are. The study falls short in developing a way to measure the dimensions of CM as well as defining the outcomes or consequences of CM on the marketer or the firm. Overall, none of the studies established a scale or define explicitly the dimension in which to measure perceived creepiness. From those previous studies, I conclude that perceived creepiness is a multi-dimensional construct and consists of a variety of inter-related attributes (Law, Wong, & Mobley, 1998), with the most pervasive being the negative feelings and emotions evoked by perceived creepiness.

Based on the data collected during my qualitative study I define perceived creepiness as "an emotional reaction to an experience, interaction, technology or unsolicited communication where personal information has been collected with your knowledge or unknowingly and used in an unexpected or surprising manner invoking negative feelings."

Using this definition of creepy along with the insights from the previous studies on perceived creepiness, I focus on the one dimension of perceived creepiness that pertains to the negative feelings and emotions associated with creepy personalized messages. Another finding in my qualitative study was that perceived creepiness and privacy intrusiveness are related but different. For example, one of the questions specifically asked, "Can you provide an example of when you were on the Internet and you felt that your privacy was invaded or violated?" 12 out of 22 respondents said "no", despite over 80% identifying themselves as "private people". When personal or private information was used in a manner in which they were not familiar or expecting, some respondents did not necessarily feel as though their privacy had been invaded or intruded upon, but described it as *creepy*,

> “It's creepy the amount of information we share online. Because again, we don't know who is on the other end of that Web site” (Professional 8).

Further,

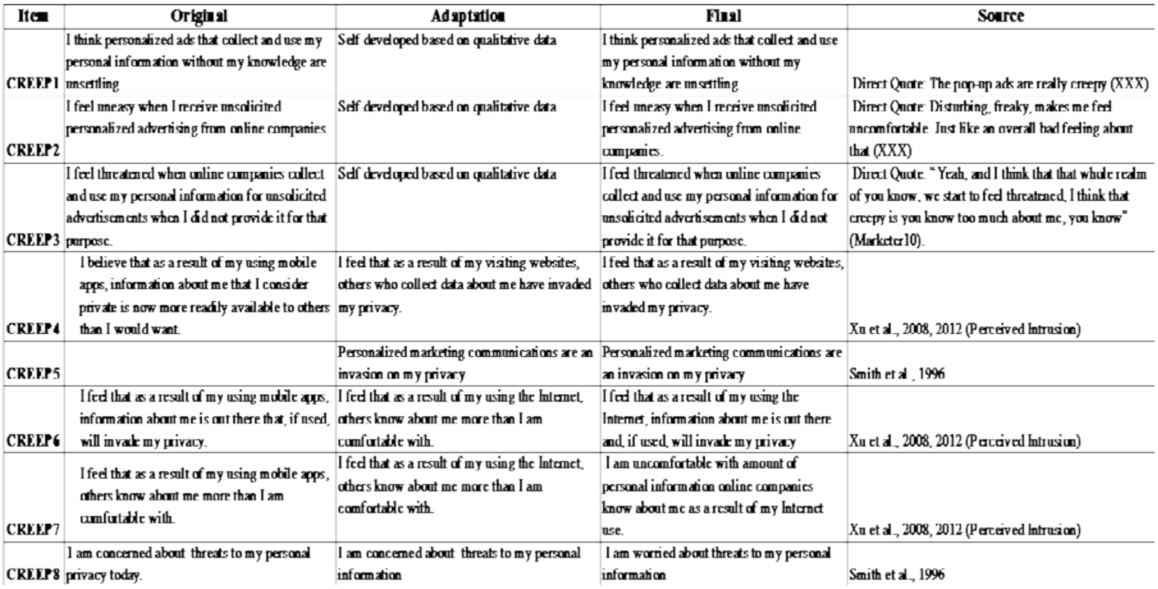
> “I didn't give them that information. I logically can't process how they got that information, so it's *creepy* in the sense that how are people getting this information, what's out there about me that I don't know about, like things that I know are out there about me are: any people search will return where I went to school or where I live or where my wedding registry is. That's not *creepy* because I don't like it, but I know why it's out there or that I can find it, but stuff that I didn't know about, about me - that's *creepy*” (Professional 13).

The data supports that *creepy* could be intrusive, but a privacy violation was not always thought to be *creepy;* thus, creepy and privacy intrusiveness are related but different even though people may respond to both perceived creepiness and privacy intrusiveness in a similar manner. Although, what messages are perceived to be creepy may change depending on the context of the message and the conditions in which the message was received, the basis of the construct and the negative feelings and emotions related to perceived creepiness should not change; which is why my scale focuses on the negative feelings associated with perceived creepiness.

2. Development of Measures

Upon completing the conceptualization phase, I then moved to the next phase prescribed by Mackenzie et al. (2011), Development of Measures, which entails generating items that represent the construct. Using the definition of perceived creepiness as a guide along with the findings from my qualitative study, I generated items that were focused solely on the dimension of perceived creepiness associated with negative feelings and emotions (affect) as that was the predominant theme gleaned from the qualitative study regarding individual’s responses toward online personalized messages. I used words and expressions that were provided during the qualitative study and were closely related to a “creepy” feeling such as eerie, unsettling or uncomfortable. Since perceived creepiness and privacy intrusiveness seemed to be related and also captured by Moore et al. (2015) in their discussion of creepy marketing, I also adapted items from existing scales that focused on the negative feelings associated with privacy intrusiveness that could readily apply to perceived creepiness. Accordingly, I developed a one-dimensional scale with eight items pertaining to the negative feelings and emotions pertaining to perceived creepiness i.e. unsettlement, uneasiness and being threatened. To ascertain the content validity of the items, three Ph.D. professors along with five Ph.D. students reviewed the items to assess word clarity, determined if the items within the scale made logical sense, determined if the wording was ambiguous or incomprehensible and clearly reflected the affect of perceived creepiness so that it would not be subject to multiple interpretations. Table D1 shows the progression of the development of the items and the source or basis for the items.

Table D1. Perceived Creepiness Scale

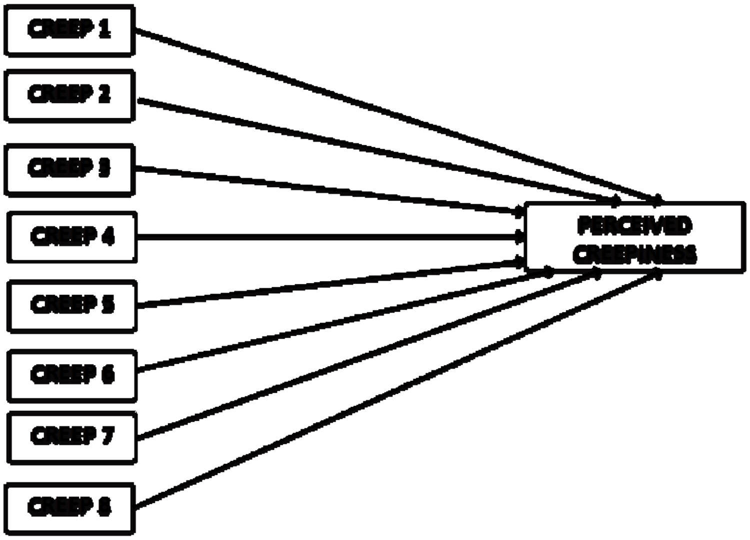


Item	Original	Adaptation	Final	Source
CREEP1	I think personalized ads that collect and use my personal information without my knowledge are unsettling	Self developed based on qualitative data	I think personalized ads that collect and use my personal information without my knowledge are unsettling	Direct Quote: The pop-up ads are really creepy (XXX)
CREEP2	I feel uneasy when I receive unsolicited personalized advertising from online companies	Self developed based on qualitative data	I feel uneasy when I receive unsolicited personalized advertising from online companies.	Direct Quote: Disturbing, freaky, makes me feel uncomfortable. Just like an overall bad feeling about that (XXX)
CREEP3	I feel threatened when online companies collect and use my personal information for unsolicited advertisements when I did not provide it for that purpose.	Self developed based on qualitative data	I feel threatened when online companies collect and use my personal information for unsolicited advertisements when I did not provide it for that purpose.	Direct Quote: “Yeah, and I think that that whole realm of you know, we start to feel threatened, I think that creepy is you know too much about me, you know” (Marketer10).
CREEP4	I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.	I feel that as a result of my visiting websites, others who collect data about me have invaded my privacy.	I feel that as a result of my visiting websites, others who collect data about me have invaded my privacy.	Xu et al., 2008, 2012 (Perceived Intrusion)
CREEP5		Personalized marketing communications are an invasion on my privacy	Personalized marketing communications are an invasion on my privacy	Smith et al., 1996
CREEP6	I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.	I feel that as a result of my using the Internet, others know about me more than I am comfortable with.	I feel that as a result of my using the Internet, information about me is out there and, if used, will invade my privacy	Xu et al., 2008, 2012 (Perceived Intrusion)
CREEP7	I feel that as a result of my using mobile apps, others know about me more than I am comfortable with.	I feel that as a result of my using the Internet, others know about me more than I am comfortable with.	I am uncomfortable with amount of personal information online companies know about me as a result of my Internet use.	Xu et al., 2008, 2012 (Perceived Intrusion)
CREEP8	I am concerned about threats to my personal privacy today.	I am concerned about threats to my personal information	I am worried about threats to my personal information	Smith et al., 1996

3. Model Specification

The next step in developing a scale (Mackenzie et al., 2011) is to formally specify the measurement model after the items generated have been determined to accurately express the dimension of the construct for which the scale is being developed. The perceived creepiness scale is a one-dimensional reflective construct in that the eight items reflect the negative affect—feelings and emotions associated with perceived creepiness. The eight items in relationship to perceived creepiness is shown in Figure D1.

Figure D1. Perceived Creepiness Items to Construct



4. Scale Evaluation and Refinement

The next step in the scale development process (Mackenzie et al., 2011) is to evaluate and refine the scale by collecting data to conduct pre-test “in order to examine psychometric properties of the scale and to evaluate its convergent, discriminant and nomological validity” (p. 310).

Measures

In addition to the newly developed perceived creepiness scale consisting of eight items to assess nomological validity, I included measurements of other constructs that would have been identified in my research that are either antecedents, consequences or in some way impact perceived creepiness and would be helpful in furthering our understanding of perceived creepiness. The other constructs included in the nomological net included online information privacy concerns (2 items), trust (5 items), perceived anonymity (5 items), control (4 items) and transparency (2 items). All items were measured using a 7-point Likert (1-Strongly Disagree to 7 – Strongly Agree) scale. By combining the perceived creepiness scale with the other constructs, I could more readily determine the relationships among the new and existing scales and also demonstrate discriminant and convergent validity.

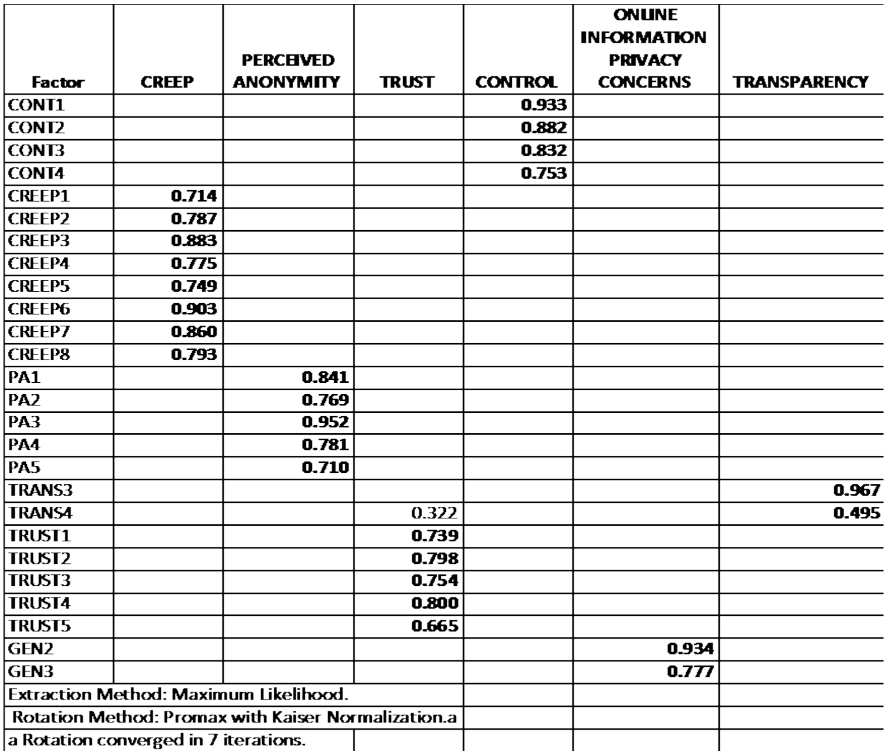
Pre-test

To test the validity of the items in the perceived creepiness scale, I recruited participants from Amazon Mechanical Turk.[26] There were 131 completed surveys, however, after cleaning the data, 106 valid responses remained. Although the sample was small, it did meet the minimum sample size of 100 to 500 respondents for an initial exploratory factor analysis (EFA) (Mackenzie, Podsakoff, & Podsakoff, 2011). Performing an EFA is one means in which to measure and show evidence of construct validity, discriminant and convergent validity as well as internal consistency (Hinkin, 1998; T. R. Hinkin, 1995)

[26] Amazon Mechanical Turk (MTurk), is an Internet crowdsourcing marketplace where requestors post jobs to complete, called a HIT (human intelligence task) and workers choose the HITs to complete for a small fee

Using SPSS statistical software (V22 and V23), I was able to review the pattern matrix, communalities, scree plot and factor loadings; and also examine reliability, Kaiser-Meyer-Olkin (KMO) and Bartlett's Test of Sphericity. I used the Maximum Likelihood extraction method since we would be using the same extraction method within AMOS where I would be conducting confirmatory factor analysis (CFA), along with Promax rotation. Kaiser-Meyer-Olkin (KMO) measure of adequacy was .889 and Bartlett's Test of Sphericity was χ^2 = 2547.039, df 325, p= .000, both indicating the appropriateness of the data for factoring and the solution was not an identity matrix (Hair et al., 2010). Based on the Pattern Matrix, shown in Table D2, the 8-item perceived creepiness scale showed convergent and discriminant validity as the eight "CREEP" items loaded strongly onto one factor; the other five constructs also loaded onto separate factors as well. One item (TRANS4) did cross-load with the Trust construct. It loaded on the Trust construct at .322 and on the Transparency construct at .495. Based on this result, I did review the statements to determine if there was any ambiguity in the statements. I decided not to remove this item as it would cause me to omit this construct. Because of the strong loadings of the other items combined with the fact that transparency appeared in the qualitative study as a dominant theme of perceived creepiness, this item will be monitored when the scale is retested with a larger sample to see how it performs. Should it remain problematic, it will be removed.

Table D2. Pattern Matrix for 8-item scale



Factor	CREEP	PERCEIVED ANONYMITY	TRUST	CONTROL	ONLINE INFORMATION PRIVACY CONCERNS	TRANSPARENCY
CONT1				0.933		
CONT2				0.882		
CONT3				0.832		
CONT4				0.753		
CREEP1	0.714					
CREEP2	0.787					
CREEP3	0.883					
CREEP4	0.775					
CREEP5	0.749					
CREEP6	0.903					
CREEP7	0.860					
CREEP8	0.793					
PA1		0.841				
PA2		0.769				
PA3		0.952				
PA4		0.781				
PA5		0.710				
TRANS3						0.967
TRANS4			0.322			0.495
TRUST1			0.739			
TRUST2			0.798			
TRUST3			0.754			
TRUST4			0.800			
TRUST5			0.665			
GEN2					0.934	
GEN3					0.777	
Extraction Method: Maximum Likelihood.						
Rotation Method: Promax with Kaiser Normalization.a						
a Rotation converged in 7 iterations.						

I also assessed reliability for each of the constructs and all exceeded the threshold of .70 (Nunnally, 1978). Cronbach's Alpha for the constructs are listed in Table D3; of most importance is the reliability measure for perceived creepiness, which was .942 for the eight items.

Table D3. Reliability Measures for Constructs

Factor Label	Cronbach's Alpha	Number of Items
OVERALL MODEL	**0.903**	**26**
Trust	0.925	5
Perceived Anonymity	0.929	5
Control	0.930	4
Online Information Privacy Concerns	0.923	2
Transparency	0.880	2
Perceived Creepiness	0.942	8

Fornell and Larcker (1981) suggest that examining composite reliability can also assess construct reliability. For the constructs, each of the composite reliability measures exceeded .70. I also examined Measures of Sampling Adequacy (MSA) across the diagonal of the anti-image matrix to ensure that they were above .70 (Dziuban & Shirkey, 1974), of which they were; values ranged from .842 to .940.

I conducted a confirmatory factor analysis (CFA), using AMOS software with Maximum Likelihood estimation to validate the established factor structure. I also examined several fit statistics, including chi-square, CFI, and RMSEA to ascertain the goodness of fit of the model and to determine if they met acceptable thresholds for an adequate fitting model (Hu & Bentler, 1995; Tabachnick & Fidell, 2007). Table D4 shows the estimates along with the significance levels of each of the items in the perceived creepiness scale.

Table D4. Perceived Creepiness Item Estimates

Item	Final	Estimates (Standardized)	Significance
CREEP1	I think personalized ads that collect and use my personal information without my knowledge are unsettling.	0.693	0.001
CREEP2	I feel uneasy when I receive unsolicited personalized advertising from online companies.	0.776	0.001
CREEP3	I feel threatened when online companies collect and use my personal information for unsolicited advertisements when I did not provide it for that purpose.	0.908	0.001
CREEP4	I feel that as a result of my visiting websites, others who collect data about me have invaded my privacy.	0.846	0.001
CREEP5	Personalized marketing communications are an invasion on my privacy.	0.797	0.001
CREEP6	I feel that as a result of my using the Internet, information about me is out there and, if used, will invade my privacy	0.851	0.001
CREEP7	I am uncomfortable with amount of personal information online companies know about me as a result of my Internet use.	0.843	0.001
CREEP8	I am worried about threats to my personal information	0.835	0.001

I also assessed construct validity by examining measures for convergent and discriminant validity. The construct met acceptable thresholds for convergent and discriminant validity as the composite ratio for all constructs exceeded .70 and AVE was greater than .50 (Fornell & Larcker, 1981), thereby, demonstrating construct validity as reflected in Table D5.

Table D5. Construct Validity Measures (N=106)

	CR (>0.70)	AVE (>0.50)	MSV	ASV
PRIV	0.923	0.858	0.386	0.088
CREEP	0.943	0.674	0.386	0.095
ANONYMITY	0.929	0.725	0.637	0.329
TRUST	0.927	0.719	0.637	0.367
CONTROL	0.931	0.773	0.523	0.265
TRANSP	0.883	0.790	0.627	0.300

Table D6 show the results of the goodness of fit measures based on the pattern matrix, from which we can conclude that the goodness of fit for the measurement model is sufficient as most of the values are within acceptable ranges of the stated thresholds (Hu & Bentler, 1995; Tabachnick & Fidell, 2007: 715). Since the sample size is small, it is expected that some of the Goodness of Fit statistics will be impacted. Because of this, we left the model as is to test with a larger sample.

Table D6. Goodness of Fit Statistics

Goodness of fit statistics	Observed Value	Recommended
Statistical		
Chi-square	408.717	
Degrees of freedom (DF)	284	
CMIN/DF	1.44	Between 1 and 3
p-value	0.000	
Relative		
CFI	0.95	>0.950
TLI	0.942	>0.950
Absolute		
SRMR	0.046	<0.05
RMSEA (90% CI)	0.065	<0.060
RMSEA (Low/High)	.050/.078	
P-Close	0.05	>0.050
AGFI	0.735	>0.90

5. Validation

During the validation step of the scale development process (Mackenzie et al., 2011), data is to be gathered from a new sample to reexamine scale properties, further assess scale validity, and cross-validate the scale. To validate the viability of the perceived creepiness scale/construct, I conducted another study, which was my primary study for using the newly developed scale. The purpose of the study was to validate factors that had been identified that led to perceived creepiness: online information privacy concerns, control, transparency, trust, perceived anonymity and perceived surveillance. I next administered an online survey, which contained twenty-one questions, eight of which were directly related to the constructs along with three scenarios in which the respondents were to assess the degree of perceived creepiness; six questions were asked to understand Internet usage and activities performed using the

Internet and three demographic questions were asked to garner age, gender and highest educational level obtained. Since we measured the independent and dependent variables within the same instrument, it was necessary to assess Common Method Bias (CMB). To test CMB, it is most appropriate to use a marker variable; therefore, we included a social desirability scale (Hays et al., 1989). A social desirability scale was selected because we assert that there is a socially desirable way to answer questions about emotions, beliefs and confidence for which we measured to some degree within the Perceived Anonymity and Online Information Privacy Concerns constructs. Using Amazon Mechanical Turk, my professional and personal network as well as social media. I received 418 responses. After removing incomplete surveys, there were 389 valid responses. Most notable is that 55% of the respondents were male and 45% were female. Median age was 37 years old and 61% had attained a Bachelor's, Master's, Professional or Doctorate degree. Eighty-five percent of the respondents spend 40 hours or less online excluding email and work related activities and 73% of the respondents have been Internet users between eleven and twenty years.

The survey item that was followed by the perceived creepiness scale was: "Please rate the following statements regarding personalized marketing communications or advertisements". As with the pre-test, I conducted an EFA, CFA and examined other psychometric values. The other constructs in the model were online information privacy concerns, trust, transparency, control, and perceived anonymity and perceived surveillance. The purpose of the EFA was to help determine if the observed variables performed as we had originally anticipated were correlated and also to determine if the minimum criteria of reliability and validity were met. We used the Principal Components

Analysis extraction method along with Promax rotation method as it is suitable for large datasets and can account for correlated factors. Following Hinkin's (1998) recommendation, the following criteria were used to determine the number of factors: eigenvalue greater than one, scree plot examination and percentage of variance explained (Cattell, 1966). I also examined factor loadings, cross-loadings, and communalities. We reviewed the communalities to determine if they met the suggested threshold, which should be above .3 (Dziuban & Shirkey, 1974). Items were retained if they had high loadings on their primary factor or low cross-loadings on another factor. Using this criteria, we eliminated several items within the online information privacy concerns construct that included, collection, use, and general privacy concerns, which contained nine items, four items (PS1 – PS4) representing Perceived Surveillance, and three items (TRANS1, TRANS2 and TRANS6) from the Transparency construct. Table D7 shows the pattern matrix.

All of the items within the Perceive Creepiness scale loaded cleanly on one factor: Creep 1 - Creep 7 ranged from .802 - .887 and Creep 8 loaded at .593.

Table D7. Pattern Matrix

PATTERN MATRIX	CREEP	TRUST	PERCEIVED ANONYMITY	CONTROL	ONLIE INFORMATION PRIVACY CONCERNS	TRANSPARENCY
CREEP1	0.867					
CREEP2	0.887					
CREEP3	0.821					
CREEP4	0.877					
CREEP5	0.878					
CREEP6	0.802					
CREEP7	0.814					
CREEP8	0.593					
TRUST1		0.791				
TRUST2		0.865				
TRUST3		0.959				
TRUST4		0.91				
TRUST5		0.793				
CONT1				0.917		
CONT2				0.95		
CONT3				0.878		
CONT4				0.705		
PRIV2					0.933	
PRIV3					0.917	
PA5			0.851			
PA6			0.83			
PA7			0.838			
PA8			0.912			
PA9			0.848			
TRANS3						0.942
TRANS4						0.918
Extraction Method: Maximum Likelihood.						
Rotation Method: Promax with Kaiser Normalization.						
Rotation converged in 7 iterations.						

I later conducted a CFA with this model and the results in Table D8 will show that the model met acceptable thresholds and had adequate fit. In this study, Cronbach’s Alpha was .936 for the 8-item scale. The other constructs in the model were trust, control, general privacy concerns, perceived anonymity, and transparency.

I examined modification indices and analyzed several fit statistics, including chi-square, CFI, and RMSEA to ascertain the goodness of fit of the model and to ensure that the measures were within suggested thresholds (Hu & Bentler, 1995; Tabachnick & Fidell, 2007: 715). CFI for the model was .969, which exceeds the recommended threshold of .950, which suggests that the hypothesized model is an adequate fit to the data. Adjusted Goodness of Fit (AGFI) was .88, slightly below the suggested threshold of .90; however, all other fit statistics were within acceptable range.

Table D8 shows the results of the goodness of fit measures (Incremental, Absolute, and Statistical) from which we can conclude that the goodness of fit for the measurement model is sufficient.

Table D8. Measurement Model – Goodness of Fit Statistics

Goodness of fit statistics	Observed Value	Recommended
Statistical		
Chi-square	539.889	
Degrees of freedom (DF)	284	
CMIN/DF	1.901	Between 1 and 3
p-value	0.000	
Relative		
CFI	0.969	>0.950
Absolute		
SRMR	0.0411	<0.05
RMSEA (90% CI)	0.048	<0.060
RMSEA (Low/High)	.042/.054	
P-Close	0.678	>0.050
AGFI	0.88	>0.90

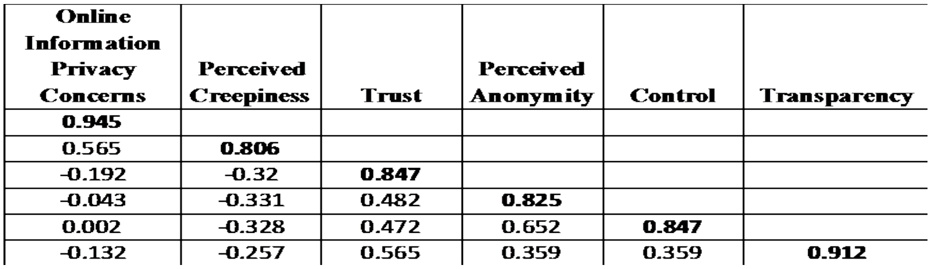
To establish validity and reliability, I used the following measures: composite reliability (CR), average variance extracted (AVE), maximum shared variance (MSV) and average shared variance (ASV). Validity and reliability measures were analyzed based on the standards of Bagozzi and Yi (1988) whereby: 1) CFA factor loadings should exceed .5 (Hair et al., 2010); 2) the composite reliability (CR) should exceed 0.7; and 3) the average variance extracted (AVE) which measures the amount of variance attributable to measurement error, should exceed 0.50 for every construct (Fornell & Larcker, 1981).

To test for convergent validity, AVE was calculated for all factors, and each factor exceeded the recommended threshold of 0.50. The composite reliability CR ranged from .908 to .943, thus exceeding the minimum threshold of 0.70, indicating reliability of the factors. To test for discriminant validity, the square root of the AVE was compared to all inter-factor correlations. Four of the six factors were below .90 (Hair et al., 2010); the other factors were .945 (Online Information Privacy Concerns) and .912 (Transparency). These results are reasonable given that these two constructs have two items, slightly below what is required for a strong construct. However, all constructs meet suggested thresholds for other validity and reliability measures. Table D9 provides a summary of the validity measures and Table D10 shows the AVE (on the diagonal) in comparison to inter-factor correlations.

Table D9. Construct Validity Measures (N=389)

Construct	CR (>0.70)	AVE (>0.50)	MSV	ASV
PRIVACY	0.943	0.893	0.319	0.075
CREEP	0.937	0.650	0.319	0.141
TRUST	0.926	0.717	0.319	0.183
ANON	0.914	0.681	0.425	0.180
CONTROL	0.908	0.718	0.425	0.177
TRANS	0.908	0.832	0.319	0.132

Table D10. AVE for Constructs (N=389)

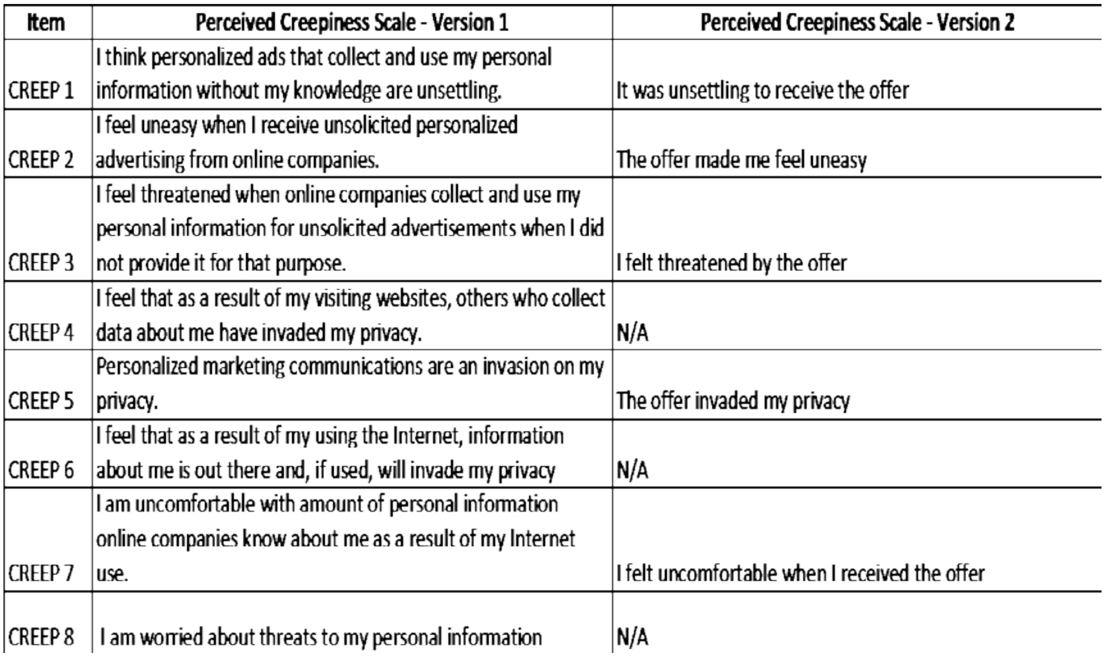


Online Information Privacy Concerns	Perceived Creepiness	Trust	Perceived Anonymity	Control	Transparency
0.945					
0.565	**0.806**				
-0.192	-0.32	**0.847**			
-0.043	-0.331	0.482	**0.825**		
0.002	-0.328	0.472	0.652	**0.847**	
-0.132	-0.257	0.565	0.359	0.359	**0.912**

Cross-Validate the Scale

I conducted a third study conducting consumer behavior experiments to test transparency, control and trust and the impact on perceived creepiness. The existing 8-item perceived creepiness scale consisted of several items that focused on the negative feelings and emotions associated with privacy intrusion, which was a dimension of perceived creepiness that was outside of the scope of my experiment; therefore, I tested a subset of the perceived creepiness scale (5 items, of which CREEP 1-3 were self-developed) that was less focused on the intrusiveness of personalized messages, because it was most appropriate for my research design. Validating the modified 5-item scale provided me with a mechanism to cross-validate a subset of the 8-item scale to some degree. However, in order to properly cross-validate the original 8-item scale, more research is needed where the perceived creepiness scale can be applied. It is not my intent to reduce or change the overall perceived creepiness scale, only to validate a subset of the scale for my research purposes. A comparison of the original and modified perceived creepiness scale used in my study is shown in Table D11.

Table D11. Comparison of Perceived Creepiness Scales



Item	Perceived Creepiness Scale - Version 1	Perceived Creepiness Scale - Version 2
CREEP 1	I think personalized ads that collect and use my personal information without my knowledge are unsettling.	It was unsettling to receive the offer
CREEP 2	I feel uneasy when I receive unsolicited personalized advertising from online companies.	The offer made me feel uneasy
CREEP 3	I feel threatened when online companies collect and use my personal information for unsolicited advertisements when I did not provide it for that purpose.	I felt threatened by the offer
CREEP 4	I feel that as a result of my visiting websites, others who collect data about me have invaded my privacy.	N/A
CREEP 5	Personalized marketing communications are an invasion on my privacy.	The offer invaded my privacy
CREEP 6	I feel that as a result of my using the Internet, information about me is out there and, if used, will invade my privacy	N/A
CREEP 7	I am uncomfortable with amount of personal information online companies know about me as a result of my Internet use.	I felt uncomfortable when I received the offer
CREEP 8	I am worried about threats to my personal information	N/A

The 5-item scale was reflective of the negative feelings and emotions associated with perceived creepiness as the 8-item scale. Since the five items were adapted to the experiment, the scale is still representative of the negative affect of perceived creepiness; the purpose of what the scale measures are unchanged. To ensure that the modified 5-item scale specifically for this study was still a valid and reliable measure, we conducted an additional test. To validate the five item perceived creepiness scale, we recruited sixty-one participants from Amazon Mechanical Turk and administered a survey that consisted of two scenarios; one that was perceived to be creepy and one that was not, followed by the modified perceived creepiness scale. The purpose of this test was to validate that the modified perceived creepiness scale actually measured changes in perceived creepiness when the influence was different, showing that the Creepy group’s perceived creepiness is discriminant from the level of perceived creepiness of the Non-Creepy group. To conduct this test, one of the following scenarios was provided to the survey participants who were randomly assigned a group by the survey host software, Qualtrics.

Creepy Scenario:

One evening, you are working on a report on your laptop made by eMaxx that you have owned for several years. Suddenly, the computer crashes. The manufacturer's warranty agreement has expired, so you did not call the Help Desk for assistance. The next morning you access your email and notice one of your messages is an offer addressed personally to you from eMaxx for a discount on a new computer. You notice another message that is from a computer repair company also addressed personally to you which states "COMPUTER CRASHED? WE CAN HELP" offering a discount for computer repair services.

Non-Creepy Scenario:

One evening, you are working on a report on your laptop made by eMaxx that you have owned for several years. Suddenly, the computer crashes. The manufacturer's warranty agreement has not expired, so you called the Help Desk for assistance. The next morning you access your email and notice one of your messages is an offer addressed personally to you from eMaxx for a discount on a new computer.

After the scenario, each respondent answered the following question, which was the 5-item Perceived Creepiness scale.

Please tell us how receiving the personalized offer from eMaxx makes you feel (7-point Likert Scale – SD to SA)

- *It was unsettling to receive the offer*
- *The offer made me feel uneasy*
- *I felt threatened by the offer*
- *The offer invaded my privacy*
- *I felt uncomfortable when I received the offer*

I performed a one-way ANOVA test that confirmed that the two groups: Creepy and Non-Creepy were significantly different from each other in terms of the level of creepiness. With this test, I was able to confirm that 1) Perceived creepiness can be measured along different levels of creepiness (F=25.561, p=.000); Cronbach's Alpha for the five-item scale was .925 and 2) Perceived level of creepiness can well distinguish between creepy and non-creepy situations. The results are shown in Table D12.

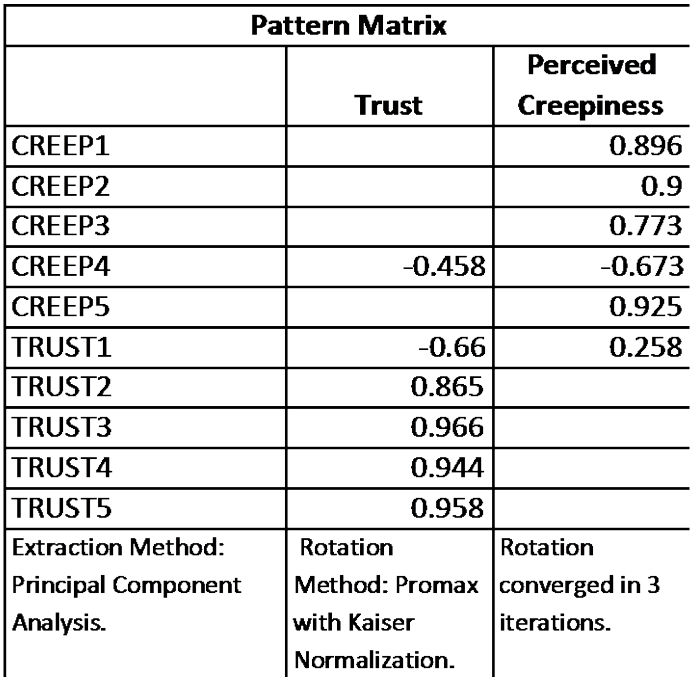
Table D12. Creepy Scale Test Results

CREEPY				
Item	**N**	**Mean**	**Significance**	**Threshold**
0 - Creepy	29	5.4552	0.000	> 5
1 - NonCreepy	32	3.4313	0.000	< 4
Total	**61**			

To further assess the discriminant and convergent validity of the modified perceived creepiness scale, another study was conducted. I conducted a pre-test with seventy-nine participants recruited from Amazon Mechanical Turk. These were not the same participants as those participating in previous pre-tests. I used a scenario to test the perceived creepiness scale in relation to the context of the message. The other construct in the test was trust as I wanted to assess the impact of consumer–firm trust on perceived creepiness. As expected, all of the Creep items loaded cleanly onto one factor. However, Creep4 was problematic as it had a negative loading, as shown in the Table D13. This item was different from the other items in the scale, as it did not deal with the negative feelings and emotions invoked by personalized messages that are perceived to be creepy, but whether the respondent felt that the offer was an invasion of privacy. Since this study was focused on transparency, control and trust and the negative feelings associated with Perceived Creepiness, this item was removed. This item should not have been a part of the modified scale as the other items in the original eight-item scale that pertained or measured intrusiveness were removed. Prior to removing Creep 4, Cronbach's Alpha was

.742; after removing Creep 4, Cronbach's Alpha improved to .943 validating that Creep 4 does not converge with the other items.

Table D13. Pattern Matrix: Creepy and Trust



Pattern Matrix		
	Trust	Perceived Creepiness
CREEP1		0.896
CREEP2		0.9
CREEP3		0.773
CREEP4	-0.458	-0.673
CREEP5		0.925
TRUST1	-0.66	0.258
TRUST2	0.865	
TRUST3	0.966	
TRUST4	0.944	
TRUST5	0.958	
Extraction Method: Principal Component Analysis.	Rotation Method: Promax with Kaiser Normalization.	Rotation converged in 3 iterations.

The 4-item scale consisted of CREEP 1, 2, 3 and 5 was next used in the third study with 238 respondents. The scale continued to be a reliable construct with a Cronbach's Alpha measurement of .953.

6. Norm Development

The final step of the scale development process (Mackenzie et al., 2011) consists of developing norms for the scale. More usage of the scale is needed to develop norms for the Perceived Creepiness scale. Some aspect of the Perceived Creepiness scale was used six times. Each time the scale or a subset of the scale was used, the results were within acceptable thresholds for reliability and validity (Hair et al., 2010; Nunnally, 1978). For the 8-item scale, the means were clustered together, and the means for the 5-

item scale were clustered together. The 4-item scale was used in only one study, so we don't have a basis for comparison.

Additional tests are needed to develop norms for the full Perceived Creepiness scale, which would be used more broadly than the modified scale that I used for a specific study. When looking at the means of all of the studies where some version of the Perceived Creepiness was used, the range was 4.17 to 5.35; this would seemingly suggest that the norm value should fall within this range, which is over a 25% difference between the lower and upper bounds. However, it is hard to draw any reliable conclusions on norms for the scale. More application of the scale and results from using the scale over time should help to produce the norms for the scale. The means for the Perceived Creepiness scale for all instances when the scale was used is shown in Table D14.

Table D14. Means of Perceived Creepiness Scale

Test	Perceived Creepiness Scale	Sample Size	Mean	Standard Deviation
Pretest 1 (Study 2)	8 items	143	5.13	1.21
Pretest 2 (Study 2)	8 items	108	5.35	1.19
Study 2	8 items	385	5.32	1.19
Revalidation of Perceived Creepiness Scale	5 items	61	4.39	1.85
Pretest (Study 3)	5 items	79	4.43	1.61
Study 3	4 items	238	4.17	1.79

Conclusion

Following the process for scale development, as prescribed by Mackenzie et al. (2011), allowed me to create a reliable scale to measure perceived creepiness. The two studies in which the scale and the resultant findings was aligned with the little that we know from the literature on perceived creepiness and what I have observed in practice and through qualitative research. As norms for the scale are developed with more use of the scale, I believe that this scale is a viable means in which to measure perceived creepiness.

REFERENCES

Adomavicius, G., & Tuzhilin, A. 2005. Personalization technologies: A process-oriented perspective. ***Communications of the ACM***, 48(10): 83–90.

Adoni, H., & Mane, S. 1984. Media and the Social Construction of Reality toward an Integration of theory and Research. ***Communication Research***, 11(3): 323–340.

Altman, I. 1975. ***The Environment and Social Behavior***. Monterey, CA: Brooks/Cole Publishing Company.

Arora, N., Dreze, X., Ghose, A., Hess, J. D., Iyengar, R., et al. 2008. Putting one-to-one marketing to work: Personalization, customization, and choice. ***Marketing Letters***, 19(3-4): 305–321.

Auspurg, K., Hinz, T., & Liebig, S. 2009. Komplexität von Lerneffekte und Plausibilität im Faktoriellen Survey Complexity , Learning Effects and Plausibility of Vignettes in the Factorial Survey Design. ***Methoden — Daten — Analysen***, 3: 59–96.

Awad, N. F., & Krishnan, M. S. 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. ***MIS Quarterly***, 30(1): 13–28.

Awad, N., & Krishnan, M. 2006. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. ***MIS Quarterly***, 30(1): 13–28.

Bagozzi, R. P., Gopinath, M., & Nyer, P. U. 1999. The role of emotions in marketing. ***Academy of Marketing Science Journal***, 27(2): 184–206.

Bagozzi, R., & Yi, Y. 1988. On the evaluation of structural equation models. ***Journal of the Academy of Marketing Science***, 16(1): 74–94.

Ball, D., Coelho, P., & Vilares, M. 2006. Service personalization and loyalty. ***Journal of Services Marketing***, 20(6): 391–403.

Bansal, G., & Gefen, D. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. ***Decision Support Systems***, 49(2): 138–150.

Barnard, L. 2014. ***The cost of creepiness: How online behavioral advertising affects consumer purchase intention***. University of North Carolina at Chapel Hill.

Baron, R., & Kenny, D. 1986. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. ***Journal of Personality and Social Psychology***, 51(6): 1173–1182.

Barth, A., Datta, A., Mitchell, J., & Nissenbaum, H. 2006. Privacy and contextual integrity: Framework and applications. ***2006 IEEE Symposium on Security and Privacy***, 15 pp. – 198. Berkeley/Oakland, CA: IEEE.

Bates, S. C., & Cox, J. M. 2008. The impact of computer versus paper-pencil survey, and individual versus group administration, on self-reports of sensitive behaviors. ***Computers in Human Behavior***, 24(3): 903–916.

Bearden, W. O., & Teel, J. E. 1983. Selected determinants of consumer satisfaction and complaint reports. ***Journal of Marketing Research***, 20(1): 21–28.

Beardsley, E. 1971. Privacy: Autonomy and selective disclosure. ***Nomos XIII: Privacy***, 56–70.

Beldad, A., De Jong, M., & Steehouder, M. 2010. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. ***Computers in Human Behavior***, 26: 857–869.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. ***The Information Society: An International Journal***, 20(January 2015): 313–324.

Benoliel, J. Q. 1996. Grounded Theory and Nursing Knowledge. ***Qualitative Health Research***, 6: 406–428.

Berger, P. L., & Luckmann, T. 1991. ***The Social Construction of Reality: A Treatise in the Sociology of Knowledge***. Penguin, UK.

Berry, L. 1995. Relationship marketing of services—growing interest, emerging perspectives. ***Journal of the Academy of Marketing Science***, 23(4): 236–245.

Bolton, R. N., & Drew, J. H. 1991. Multistage Model of of Service Customers ’ Quality and Value Assessments. ***Journal of Consumer Research***, 17(4): 375–384.

Bratman, B. 2001. Brandeis and Warren’s The Right to Privacy and the Birth of the Right to Privacy. ***Tennessee Law Review***, 69: 623.

Bruening, P., & Culnan, M. J. 2015. Through a Glass Darkly: From Privacy Notices to Effective Transparency. ***North Carolina Journal of Law and …***.

Buchanan, T., & Paine, C. 2007. Development of measures of online privacy concern and protection for use on the Internet. ***Journal of the American Society for Information Science and Technology***, 58(2): 157–165.

Buhrmester, M., Kwang, T., & Gosling, S. D. 2011. Amazon’s Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data? ***Perspectives on Psychological Science***, 6(1): 3–5.

Buhrmester, M., Kwang, T., & Gosling, S. D. 2011. Amazon's Mechanical Turk. ***Perspectives on Psychological Science***, 6(1): 3–5.

Cadotte, E. R., Woodruff, R. B., & Jenkins, R. L. 1987. Expectations and norms in models of consumer satisfaction. ***Journal of Marketing Research***, 305–314.

Camarinha-Matos, L., & Goes, J. 2013. Contributing to the Internet of Things. In L. M. Camarinha-Matos, S. Tomic, & P. Graça (Eds.), ***Technological Innovation for the Internet of Things***: 3–12. Springer.

Cattell, R. B. 1966. The Scree Test For The Number Of Factors. ***Multivariate Behavioral Research***, 1(2): 245–276.

Cebrzynski, G., & Shermach, K. 1993. Summary of `1992 Harris-Equifax. ***Marketing News***, 27(17).

Cellan-Jones, R. 2014. Stephen Hawking warns artificial intelligence could end mankind. ***bbc.com***.

Chaminade, T. 2007. Anthropomorphism influences perception of computer-animated characters' actions. ***Social Cognitive and Affective Neuroscience***, 2(3): 206–216.

Charmaz, K. 1995. Grounded Theory. (J. A. Smith, R. Harre, & L. Van Langenhove, Eds.)***Rethinking methods in psychology***. SAGE Publications.

Charmaz, K. 2003. Grounded theory. ***Strategies of Qualitative Inquiry***, 22: 124–127.

Charmaz, K. 2006a. ***Constructing grounded theory: A practice guide through qualitative analysis***. London: SAGE Publications.

Charmaz, K. 2006b. Reconstructing theory in grounded theory studies. ***Constructing Grounded Theory***: 123–150.

Chellappa, R. K., & Sin, R. G. 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. ***Information Technology and Management***, 6(2-3): 181–202.

Christopherson, K. M. 2007. The positive and negative implications of anonymity in Internet social interactions: "On the Internet, nobody knows you're a dog." ***Computers in Human Behavior***, 23(6): 3038–3056.

Chui, M., Loffler, M., & Roberts, R. 2010. The Internet of Things. ***McKinsey Quarterly***. http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things.

Churchill, G. A. 1982. An investigation into the determinants of customer satisfaction. ***Carol Surprenant JMR Journal of Marketing Research Nov***, 19(000004): 1986–

491.

Churchill Jr., G. a. 1979. A paradigm for developing better measures of marketing constructs. ***Journal of Marketing Research***, 16(1): 64–73.

Clarke, R. 1999. Internet privacy concerns confirm the case for intervention. ***Communications of the ACM***, 42(2): 60–67.

Clemmer, E., & Schneider, B. 1996. Fair service. ***Advances in Services Marketing and Management***, 5: 109–126.

Cochran, P., Tatikinda, M. V., & Magid, J. M. 2007. Radio Frequency Identification and the Ethics of Privacy. ***Organizational Dynamics***, 36(2): 217–229.

Cohen, J. 2008. Privacy, visibility, transparency, and exposure. ***The University of Chicago Law Review***, 75(1): 185–201.

Corbin, J. M., & Strauss, A. 1990. Grounded theory research: Procedures, canons, and evaluative criteria. ***Qualitative Sociology***, 13: 3–21.

Corbitt, B. J., Thanasankit, T., & Yi, H. 2003. Trust and e-commerce: A study of consumer perceptions. ***Electronic Commerce Research and Applications***, 2(3): 203–215.

Corley, K., & Gioia, D. 2011. Building theory about theory building: what constitutes a theoretical contribution? ***Academy of Management Review***, 36(1): 12–32.

Creswell, J. 2003. Advanced mixed methods research designs. ***Handbook of Mixed …***.

Creswell, J., & Plano Clark, V. 2011. Designing and conducting mixed-methods research. ***The Sage handbook of qualitative research***.

Cukier, K., & Mayer-Schoenberger, V. 2013. The Rise of Big Data. ***Foreign Affairs***.

Culnan, M. J. 1993. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. ***MIS Quarterly***, 17(3): 341–363.

Culnan, M. J. 1995. Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing. ***Journal of Direct Marketing***, 9: 10–19.

Culnan, M. J., & Armstrong, P. K. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. ***Organization Science***, 10(1): 104–115.

Culnan, M. J., & Bies, R. 2003. Consumer privacy: Balancing economic and justice considerations. ***Journal of Social Issues***, 59(2): 323–342.

Dapko, J. L. 2012. ***Perceived firm transparency: Scale and model development***. University of South Florida.

Dator, J. 2009. ***Age Cohort Analysis***. Available from www.futures.hawaii.edu.

Dinev, T., & Hart, P. 2002. Internet privacy concerns and trade-off factors: empirical study and business implications. ***International Conference On Advances In Infrastructure for E-Business***.

Dinev, T., & Hart, P. 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. ***Behaviour & Information Technology***, 23(6): 413–422.

Dinev, T., & Hart, P. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. ***Information Systems Research***, 17(1): 61–80.

Dinev, T., Hart, P., & Mullen, M. R. 2008. Internet privacy concerns and beliefs about government surveillance – An empirical investigation. ***The Journal of Strategic Information Systems***, 17(3): 214–233.

Doney, P. M., & Cannon, J. P. 1997. An examination of the nature of trust in buyer-seller relationships. ***The Journal of Marketing***, 61(2): 35–51.

Dooley, R. 2012. Forget Evil, Don't Be Creepy. ***neurosciencemarketing.com***.

Double Click Website. 2011. ***DoubleClick Website***.

Downes, L. 2012. Customer Intelligence, Privacy, and the "Creepy Factor" - Larry Downes - Harvard Business Review. ***Harvard Business Reveiw***. http://blogs.hbr.org/2012/08/customer-intelligence-privacy/.

Dunfee, T. W., Smith, N. C., & Ross Jr., W. T. 1999. Social Contracts and Marketing Ethics. ***Journal of Marketing***, 63(3): 14–32.

Dziuban, C. D., & Shirkey, E. C. 1974. When is a correlation matrix appropriate for factor analysis? Some decision rules. ***Psychological Bulletin***, 81(6): 358–361.

Eggert, A., & Helm, S. 2003. Exploring the impact of relationship transparency on business relationships A cross-sectional study among purchasing managers in Germany. ***Industrial Marketing Management***, 32: 101–108.

Emerson, R. 1976. Social exchange theory. ***Annual Review of Sociology***, 2: 335–362.

Equifax :: Consumers :: Privacy Survey. n.d. . http://www.frogfire.com/frogfire_archive/equifax/consumers/privacy_survey/privacy_survey.html.

Estes, A. C. 2013. The NSA's Elite Hacker Squad Is Suffering in the Post-Snowden Era. ***Gizmodo***. http://gizmodo.com/the-nsas-elite-hacker-squad-is-suffering-in-the-post-s-1446367592.

Federal Trade Commission. 2014. Data brokers: A call for transparency and accountability. ***… . ftc. gov/system/files/documents/reports/data-brokers- …***. Available from www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountabilityreport-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Folger, R., & Greenberg, J. 1985. Procedural justice: An interpretive analysis of personnel systems. ***Research in Personnel and Human Resources Management***, 3(1): 141–183.

Folkes, V. S. 1988. Recent Attribution Research in Consumer Behavior: A Review and New Directions. ***Journal of Consumer Research***, 14(4): 548.

Fornell, C., & Larcker, D. F. 1981. Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. ***Journal of Marketing Research***, 18(3): 382–388.

Forrester Research, Inc. 2010. ***North American Technographics® Interactive Marketing Online Benchmark Recontact Survey, Q2 2010 (US)***.

Foxman, E. R., & Kilcoyne, P. 1993. Information technology, marketing practice, and consumer privacy: Ethical issues. ***Journal of Public Policy & Marketing***, 12(1): 106–119.

Fried, C. 1990. Privacy: A rational context. ***Computers, Ethics, & Society***.

Friend, C. 2004. Social Contract Theory. ***Internet Encyclopedia of Philosophy***, 97: 139–155.

Garbarino, E., & Johnson, M. S. 1999. The different roles of satisfaction, trust, and commitment in customer relationships. ***Journal of Marketing***, 63(2): 70–87.

Gavison, R. 1980. Privacy and the Limits of Law. ***The Yale Law Journal***.

Gebler, D. 2012. ***The 3 Power Values: How Commitment, Integrity, and Transparency Clear the Roadblocks to Performance***. John Wiley & Sons.

Gellman, R. 2014. Fair information practices: A basic history. ***Available at SSRN 2415020***.

GfK. 2014. ***New GfK US Survey Reveals Growing Concerns over Data Privacy, Desire for Corporate and Government Action***. Available from http://www.gfk.com/insights/press-release/new-gfk-us-survey-reveals-growing-concerns-over-data-privacy-desire-for-corporate-and-government-action-1/.

Giddens, A. 1984. ***The constitution of society***. Berkeley, CA: University of California Press.

Gioia, D. a., Corley, K. G., & Hamilton, a. L. 2012. Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. ***Organizational Research Methods***, 16(1): 15–31.

Gioia, D. a., & Pitre, E. 1990. Multiparadigm Perspectives on Theory Building. ***Academy of Management Review***, 15(4): 584–602.

Glaser, B. G., & Strauss, A. L. 1967. The discovery of grounded theory. ***International Journal of Qualitative Methods***, vol. 5.

Glaser, B., & Strauss, A. 1967. Grounded Theory: The Discovery of Grounded Theory. ***Sociology The Journal Of The British Sociological Association***, vol. 12.

Goodwin, C. 1991. Privacy: recognition of a consumer right. ***Journal of Public Policy & Marketing***.

Google. n.d. ***Google Glass***. http://www.google.com/glass/start/.

Guilford, J., Christensen, P., & Bond, N. 1954. ***DF opinion survey***.

Gustafsson, A., Johnson, M. D., & Roos, I. 2005. The effects of customer satisfaction, relationship commitment dimensions, and triggers on customer retention. ***Journal of Marketing***, 69(4): 210–218.

Gwinner, K. 1997. A model of image creation and image transfer in event sponsorship. ***International Marketing Review***, 14(3): 145–158.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. 2010. ***Multivariate data analysis*** (7th ed.). Upper Saddle River, NJ: Pearson Prentice-Hall.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. 2009. ***Multivariate Data Analysis***. Prentice Hall.

Hair, J., Ringle, C., & Sarstedt, M. 2013. Editorial-partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. ***Long Range Planning***.

Hays, R. D., Hayashi, T., & Stewart, a. L. 1989. A Five-Item Measure of Socially Desirable Response Set. ***Educational and Psychological Measurement***.

Hechter, M., Kim, H., & Baer, J. 2005. Prediction versus explanation in the measurement of values. ***European Sociological Review***, 21(2): 91–108.

Helft, M., & Vega, T. 2010. Retargeting Ads Follow Surfers to Other Sites. ***The New York Times***. http://cacm.acm.org/news/98282-retargeting-ads-follow-surfers-to-other-sites/fulltext.

Herring, S. 1994. ***Gender differences in computer mediated communication: bringing familiar baggage to the new frontier, keynote talk***. Miami, FL: American Library Association annual convention, Miami, FL, June 27. “Making the Network: Is There Gender in Communication?” panel discussion.

Hill, K. 2012. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did - Forbes. ***Forbes***. http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

Hinkin, T. R. 1995. A Review of Scale Development Practices in the Study of Organizations. ***Journal of Management***, 21(5): 967–988.

Hinkin, T. R. 1995. A Review of Scale Development Practices in the Study of Organizations. ***Journal of Management***, 21(5): 967–988.

Hinkin, T. R. 1998. A brief tutorial on the development of measures for use in survey questionnaires. ***Organizational Research Methods***, 1(1): 104–121.

Hosmer, L. T. 1995. Trust: The Connecting Link Between Organizational Theory and Philosophical Ethics. ***Academy of Management Review***, 20(2): 379–403.

Hu, L., & Bentler, P. 1995. Evaluating Model Fit. ***Structural Equation Modeling. Concepts, Issues, and Applications***: 76–99.

Hughes, R. 1998. Considering the vignette technique and its application to a study of drug injecting and HIV risk and safer behaviour. ***Sociology of Health & Illness***.

Hunter, L. 1995. Public image. ***Computers, Ethics and Social Values. Prentice Hall, …***.

Izard, C. E. 1977. ***Human Emotions***. New York: Plenum.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. 2003. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. ***Journal of Consumer Research***, 30(2): 199–218.

Jasso, G. 1988. Whom Shall We Welcome? Elite Judgments of the Criteria for the Selection of Immigrants. ***American Sociological Review***, 53(6): 919.

Jasso, G. 2006. Factorial Survey Methods for Studying Beliefs and Judgments. ***Sociological Methods & Research***, 34(3): 334–423.

Johnson, M. D., & Auli, S. 1998. Customer Satisfaction, Loyalty, and the Trust Environment. ***Advances in Consumer Research***, 25(1): 15–20.

Jøsang, A., & Tran, N. 2000. Trust Management for E-commerce. ***Proceedings Virtual Banking***.

Karvounis, N. 2012. What Should You Tell Customers About How You're Using Data. ***Harvard Business Reveiw***.

Katz, J. E., & Tassone, A. R. 1990. Public Opinion Trends: Privacy and Information Technology. ***Public Opinion Quarterly***, 54: 125–143.

Keenan, T. P. 2014. ***Technocreep***. Singapore Books.

Kehoe, C., Pitkow, J., & Morton, K. 1997. ***Eighth WWW User Survey***. [on-line web page]. http://www.cc.gatech.edu/gvu/user_surveys/survey-1997-04/.

Kelty, C. 2005. Geeks, Social Imaginaries, and Recursive Publics. ***Cultural Anthropology***, 20(2): 185–214.

Kelvin, P. 1973. A Social-Psychological Examination of Privacy. ***British Journal of Social and Clinical Psychology***, 12: 248–261.

Kosack, S., & Fung, A. 2014. Does transparency improve governance? ***Annual Review of Political Science***.

Kotsko, A. 2015. ***Creepiness***. Zero Books.

Kramer, I. 1989. Birth of Privacy Law: A Century since Warren and Brandeis, The. ***Cath. UL Rev.***

Kuhlman, L. 2011. ***Pride & prejudice and zombies: an exercise in postmodernism***.

Lattman, P. 2007. The Origins of Justice Stewart's "I Know It When I See It" - Law Blog - WSJ. ***Wall Street Journal***. http://blogs.wsj.com/law/2007/09/27/the-origins-of-justice-stewarts-i-know-it-when-i-see-it/.

Laufer, R. S., & Wolfe, M. 1977. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. ***Journal of Social Issues***, 33: 22–42.

Law, K. S., Wong, C. S., & Mobley, W. H. 1998. Toward a taxonomy of multidimensional constructs. ***Academy of Management Review***, 23(4): 741–755.

Lewicki, R. J., McAllister, D. J., & Bies, R. I. 1998. Trust and distrust: New relationships and realities. ***Academy of Management Review***, 23(3): 438–458.

Lind, E., & Tyler, T. 1988. ***The social psychology of procedural justice***.

Lohr, S. 2015. If Algorithms Know All, How Much Should Humans Help? ***www.nytimes.com***.

Lynham, S. A. 2002. The General Method of Theory-Building Research in Applied Disciplines. ***Advances in Developing Human Resources***, 4(3): 221–241.

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. 2011. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. ***MIS Quarterly***, 35(2): 293–334.

Madden, M. 2014a. ***Public Perceptions of Privacy and Security in the Post-Snowden Era***. Pew Research Center, November 12, 2014. Available from http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

Madden, M. 2014b. ***Public Perceptions of Privacy and Security in the Post-Snowden Era***.

Madden, M., Fox, S., Smith, A., & Vitak, J. 2007. ***Digital Footprints: Online identity management and search in the age of transparency***.

Malhotra, N. K., Kim, S. S., & Agarwal, J. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. ***Information Systems Research***.

Manjoo, F. 2012. ***The uncanny valley of internet advertising***. The Slate Group, August 23, 2012. Available from http://www.slate.com/articles/technology/technology/2012/08/the_uncanny_valley_of_internet_advertising_why_do_creepy_targeted_ads_follow_me_everywhere_i_go_on_the_web_.html.

Mankell, H. 2011. ***The Troubled Man***.

Mano, H., & Oliver, R. L. 1993. Assessing the Dimensionality and Structure of the Consumption Experience: Evaluation, Feeling, and Satisfaction. ***Source Journal of Consumer Research***, 20(3): 451–466.

Margulis, S. T. 1977. Conceptions of Privacy: Current Status and Next Steps. ***Journal of Social Issues***, 33: 5–21.

Martin, K. E. 2012. Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. ***Journal of Business Ethics***.

Martin, M., Stadler, C., Frischmuth, P., & Lehmann, J. 2014. Increasing the financial transparency of european commission project funding. ***Semantic Web***.

Mason, R. O., Mason, F. M., & Culnan, M. J. 1995. ***The ethics of information management***. Thousand Oaks, CA: Sage.

Mason, W., & Suri, S. 2012. Conducting behavioral research on Amazon's Mechanical Turk. ***Behavior Research Methods***, 44(1): 1–23.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. 1995. An integrative model of organizational trust. ***Academy of Management Review***, 20(3): 709–734.

McAndrew, F., & Koehnke, S. n.d. Basis of a poster presented at the annual meeting of the Society for Personality and Social Psychology, New Orleans, January, 2013. ***Academia.edu***.

McKnight, D. 1998. Initial trust formation in new organizational relationships. ***Academy of Management …***.

Merriam-Webster. 2012. MERRIAM-WEBSTER'S ONLINE DICTIONARY. ***Merriam-Webster***. http://www.merriam-webster.com/.

Metzger, M. J. 2007. Communication Privacy Management in Electronic Commerce. ***Journal of Computer-Mediated Communication***, 12: 335–361.

Miller, A. 1971. ***The assault on privacy: computers, data banks, and dossiers***.

Milne, G., & Culnan, M. 2002. Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 US Web surveys. ***The Information Society***.

Milne, G., & Gordon, M. 1993. Direct mail privacy-efficiency trade-offs within an implied social contract framework. ***Journal of Public Policy & Marketing***.

Milne, G., Rohm, A., & Bahl, S. 2004. Consumers' protection of online privacy and identity. ***Journal of Consumer Affairs***.

Mittal, B., & Lassar, W. M. 1996. The role of personalization in service encounters. ***Journal of Retailing***, 72(1): 95–109.

Miyazaki, A. D. 2008. Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. ***Journal of Public Policy & Marketing***.

Montgomery, A., & Smith, M. D. 2008. Prospects for Personalization on the Internet. ***Journal of Interactive Marketing***, 23(2): 130–137.

Moor, J. 1990. The ethics of privacy protection. ***Library Trends***.

Moor, J. H. 1997. Towards a Theory of Privacy in the Information Age. ***Computers and Society***.

Moore, R., Moore, M., Shanahan, K., Horky, A., & Mack, B. 2015. Creepy marketing: Three dimensions of perceived excessive online privacy violation. ***Marketing Management Journal***, 25(1): 43–53.

Moorman, C., Zaltman, G., & Deshpande, R. 1992. Relationships Between Providers and

Users of Market Research: The Dynamics of Trust Within and Between Organizations. ***Journal of Marketing Research (JMR)***, 29(3): 314–328.

Morgan, R., & Hunt, S. 1994. The commitment-trust theory of relationship marketing. ***The Journal of Marketing***.

Mori, M. 1970. The Uncanny Valley. ***Energy***, 7(4): 33–35.

Mori, M., MacDorman, K. F., & Kageki, N. 2012. The uncanny valley. ***IEEE Robotics and Automation Magazine***, 19(2): 98–100.

Morimoto, M., & Macias, W. 2009. A conceptual framework for unsolicited commercial e-mail: Perceived intrusiveness and privacy concerns. ***Journal of Internet Commerce***.

New Oxford American Dictionary. 2016. ***“Context” definition***. Oxford University Press.

Nissenbaum, H. 2004. Privacy as contextual integrity. ***Wash. L. Rev.***, 101–139.

Nissenbaum, H. 2009. ***Privacy in context: Technology, policy, and the integrity of social life***. Stanford, CA: Stanford University Press.

Nowak, G., & Phelps, J. 1992. Understanding privacy concerns. An assessment of consumers’ information-related knowledge and beliefs. ***Journal of Direct Marketing***.

Nunnally, J. 1978. ***Psychometric methods***. New York, NY: McGraw-Hill.

OECD. 1970. Guidelines on the Protection of Privacy andTransborder Flows of Personal Data. ***www.oecd.org***.

Oliver, R. 1981. Measurement and evaluation of satisfaction processes in retail settings. ***Journal of Retailing***.

Oliver, R. L. 1983. Cognitive, Affective, and Attribute of the Satisfaction Response. ***Churchill and Surprenant Oliver***.

Oliver, R. L. 1993. Cognitive, Affective, and Attribute Bases of the Satisfaction Response. ***Journal of Consumer Research***, 20(3): 418.

Oliver, R. L., & DeSarbo, W. S. 1988. Response Determinants in Satisfaction Judgments. ***Journal of Consumer Research***, 14(4): 495.

Oliver, R. L., & Swan, J. E. 1989. Equity and Disconfirmation Perceptions as Influences on Merchant and Product Satisfaction. ***Journal of Consumer Research***, 16(3): 372.

Ong, J. 2012. ***Orbitz displaying higher-priced hotels to Macs versus PCs***. http://appleinsider.com/articles/12/06/25/orbitz_displaying_higher_priced_hotels_to _macs_than_pcs.

Orwell, G. 1986. 1984 Nineteen Eighty-Four. ***The Modern Language Review***, 81(4): 994.

Parent, W. 1983. Privacy, Morality & The Law. ***Philosophy & Public Affairs***, 12(No. 4 Autumn).

Pavlou, P. A. 2011. State of the Information Privacy Literature: Where Are We Now and Where Should We Go? ***MIS Quarterly***, 35(4): 977–988.

Petronio, S. 2002. Communication Privacy Management Theory. ***Boundaries of Privacy: Dialectics of Disclosure***, (April): 168–180.

Petronio, S. 2010. Communication privacy management theory: What do we know about family privacy regulation? ***Journal of Family Theory & Review***, 2(3): 175–196.

Petronio, S., & Durham, W. T. 2008. Communication privacy management theory. In Leslie A. Baxter & Dawn O. Braithwaite (Eds.), ***Engaging theories in interpersonal communication: Multiple perspectives***: 309–322. Sage.

Phelps, J., Nowak, G., & Ferrell, E. 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. ***Journal of Public Policy & Marketing***, 19(1): 27–41.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. ***Journal of Applied Psychology***, 88(5): 879–903.

Posner, R. 1978. An Economic Theory of Privacy. ***AEA Papers and Proceedings***, 71: 19 – 26.

Prensky, M. 2001. Digital natives, digital immigrants part 1. ***On the Horizon***, 9(5): 1–6.

Professorgrossman.com, & Inter-Act, 13th Edition. n.d. ***Disclosure and Privacy.ppt***. https://www.google.com/?gfe_rd=ssl&ei=NHH1VpSIOYHM8AewoJCQCA#q=Grossman%2C+Disclosure+and+Privacy.ppt, March 25, 2016.

PwC. 2013. ***The Speed of Life: Consumer Intelligence Series***.

Rachels, J. 1975. Why privacy is important. ***Philosophy & Public Affairs***.

Rawls, J. 1999. ***A theory of justice***. Harvard University Press.

Reichheld, F. F. 2003. The one number you need to grow. ***Harvard Business Review***, 81(12): 46–54, 124.

Reichheld, F. F., & Schefter, P. 2000. E-Loyalty. ***Harvard Business Review***, 78(August):

105–113.

Renold, E. 2002. Using vignettes in qualitative research. ***Building Research Capacity***.

Rohm, A., & Milne, G. 2004. Just what the doctor ordered: the role of information sensitivity and trust in reducing medical information privacy concern. ***Journal of Business Research***.

Roper Center for Public Opinion Research. 1998. ***On-line web page. http://www.ropercenter.uconn.edu***.

Russell, J. a. 1979. Affective space is bipolar. ***Journal of Personality and Social Psychology***, 37(3): 345–356.

Schnackenberg, A. K., & Tomlinson, E. C. 2014. Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. ***Journal of Management***, [online]: 1–27.

Schneider, B., & Bowen, D. E. . 1995. Winning the Service Game. ***Harvard Business School Press***, 103–107.

Schoenbachler, D. D., & Gordon, G. L. 2002. Trust and customer willingness to provide information in database-driven relationship marketing. ***Journal of Interactive Marketing***, 16(3): 2–16.

Selinger, E. 2012. Why Do We Love to Call New Technologies Creepy? ***Slate***.

Shankar, V., Smith, A. K., & Rangaswamy, A. 2003. Customer satisfaction and loyalty in online and offline environments. ***International Journal of Research in Marketing***, 20(2): 153–175.

Sheehan, K. B. 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviors. ***Journal of Interactive Marketing***, 13(4): 24–38.

Sheehan, K. B. 2002. Toward a Typology of Internet Users and Online Privacy Concerns. ***The Information Society***.

Sheehan, K. B., & Hoy, M. G. 2000. Dimensions of Privacy Concern Among Online Consumers. ***Journal of Public Policy & Marketing***, 19(1): 62–73.

Sheehan, K., & Hoy, M. 1999a. Flaming, complaining, abstaining: How online users respond to privacy concerns. ***Journal of Advertising***.

Sheehan, K., & Hoy, M. 1999b. Using e -mail to survey Inte
States: Methodology and assessment. ***Journal of Computer .-Mediated*** ···

Simitis, S. 1987. Reviewing privacy in an information society. ***University of***

Pennsylvania Law Review.

Singer, N. 2013. Acxiom Lets Consumers See Data It Collects. ***Nytimes.com***. http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html?pagewanted=all&_r=0.

Sirdeshmukh, D., Singh, J., & Sabol, B. 2002. Consumer trust, value, and loyalty in relational exchanges. ***Journal of Marketing***, 66(1): 15–37.

Smith, H. J., Dinev, T., & Xu, H. 2011. Information privacy research: an interdisciplinary review. ***MIS Quarterly***, 35: 989–1016.

Smith, H., Milberg, S., & Burke, S. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. ***MIS Quarterly***, 20: 167–196.

Solove, D. 2006. A taxonomy of privacy. ***University of Pennsylvania Law Review***, 154: 477–560.

Spector, N. 2012. Be relevant, not creepy - Direct Marketing News. ***DM News***. http://www.dmnews.com/be-relevant-not-creepy/article/256050/.

Sprenger, P. 1999. Sun on Privacy: "Get Over It." ***Wired***. http://www.wired.com/politics/law/news/1999/01/17538.

Staples, B., & Field, T. 2013. Questioning the Culture of Surveillance - BankInfoSecurity. ***Bank InfoSecurity***. http://www.bankinfosecurity.com/interviews/questioning-culture-surveillance-i-2117.

Stein, J., & Harrell, E. 2011. Your Data, Yourself. ***Time Magazine***.

Stevens, A. 2014. ***What is "creepy"? Towards understanding that eerie feeling when it seems the internet "knows" you***. Qualitative Research Report, Doctor of Management, Case Western Reserve University, Cleveland, OH.

Stevens, A. 2015. ***Demystifying creepy marketing communications***. Quantitative Research Report, Doctor of Management, Case Western Reserve University, Cleveland, OH.

Stevens, R. P. 2002. Can Database Marketing Avoid the Creep Factor? ***DM News***.

Stewart, P. 1964. Jacobellis v Ohio. ***US Rep***.

Strauss, A., & Corbin, J. 1998. Grounded Theory Designs. ***Basics of qualitative research: Techniques and procedures for developing grounded theory***.

Strauss, A., & Corbin, J. 2008. Strauss, A., & Corbin, J. (1990). ***Basics of qualitative***

research: Grounded theory procedures and techniques. Newbury, vol. 3.

Strauss, A. L. 1987. Qualitative analysis for social scientists. ***World***, vol. 1.

Swanson, R. A., & Chermack, T. J. 2013. ***Theory building in applied disciplines***. Berrett-Koehler Publishers.

Tabachnick, B. G., & Fidell, L. S. 2007. Using Multivariate Statistics. ***PsycCRITIQUES***, vol. 28.

Tashakkori, A., & Teddlie, C. 2010. ***Sage handbook of mixed methods in social & behavioral research***.

Tavani, H. T. 2007. Philosophical theories of privacy: Implications for an adequate online privacy policy. ***Metaphilosophy***, 38(1): 1–22.

Taylor, C. 2002. Modern Social Imaginaries. ***Public Culture***, 14(1): 91–124.

Taylor, D. G., Davis, D. F., & Jillapalli, R. 2009. Privacy Concern and Online Personalization: The Moderating Effects of Information Control and Compensation. ***Electronic Commerce Research***, 93: 203–223.

Teddlie, C., & Tashakkori, A. 2009. ***Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences***.

Tene, O., & Polonetsky, J. 2012. Privacy in the Age of Big Data: A Time for Big Decisions. ***Stanford Law Review Online***, 64: 63.

Tene, O., & Polonetsky, J. 2013. A Theory of Creepy: Technology, Privacy and Shifting Social Norms. ***Yale Journal of Law & Technology***, 16(1): 1–32.

Thierer, A. 2013. The pursuit of privacy in a world where information control is failing. ***Harvard Journal of Law and Public Policy***, 36(2): 409–455.

Truste Privacy Index. 2012. .

TRUSTe/National Cyber Security Alliance. 2016. ***TRUSTe/NCSA Consumer Privacy Index***. Available from https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/.

Tse, D., & Wilton, P. 1988. Models of consumer satisfaction formation: an extension. ***Journal of Marketing***, 25(May): 204–212.

U.S. Consumer Findings from Online and Mobile Privacy Perceptions Report. 2012. ***Truste Press Release***. http://www.truste.com/about-TRUSTe/press-room/news_truste_releases_us_customer_findings_report.

Ur, B., Leon, P. L., Cranor, L. F., Shay, R., & Wang, Y. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. ***SOUPS 2012***.

Urban, G. L., Amyx, C., & Lorenzon, A. 2009. Online Trust: State of the Art, New Frontiers, and Research Potential. ***Journal of Interactive Marketing***, 23(2): 179–190.

Urban, G. L., Sultan, F., & Qualls, W. J. 2000. Placing Trust at the Center of Your Internet Strategy. ***Sloan Management Review***, 42(1): 39–48.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. 2006. Concern for information privacy and online consumer purchasing. ***Ournal of the Association for Information Systems***, 7(1): 16.

Von Drehle, D. 2013. The Surveillance Society. ***nation.time.com***.

Wallander, L. 2009. 25 years of factorial surveys in sociology: A review. ***Social Science Research***, 38(3): 505–520.

Wang, P., & Petrison, L. a. 1993. Direct marketing activities and personal privacy.A consumer survey. ***Journal of Direct Marketing***, 7(1): 7–19.

Ware, W. 1973. ***Records, computers and the rights of citizens***.

Warren, S. D., & Brandeis, L. D. 1890. The right to privacy. ***Harvard Law Review***, 4: 193–220.

Watson, S. M. 2014. ***Data doppelgängers and the uncanny valley of personalization***. The Atlantic Monthly Group, June 16, 2014. Available from http://www.theatlantic.com/technology/archive/2014/06/data-doppelgangers-and-the-uncanny-valley-of-personalization/372780/.

Waytz, A., & Morewedge, C. 2010. Making sense by making sentient: effectance motivation increases anthropomorphism. ***Journal of Personality …***.

Westbrook, R. A. 1987. Product/Consumption-Based Affective Responses and Postpurchase Processes. ***Source Journal of Marketing Research***, 24(3): 258–270.

Westbrook, R. A., & Oliver, R. L. 1991a. The Dimensionality of Consumption Emotion Patterns and Consumer Satisfaction. ***Journal of Consumer Research***, 18(1).

Westbrook, R. A., & Oliver, R. L. 1991b. The Dimensionality of Consumption Emotion Patterns and Consumer Satisfaction. ***Source Journal of Consumer Research***, 18(1): 84–91.

Westin, A. 1966. Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy. ***Columbia Law Review***.

Westin, A. 1968. Privacy and freedom. ***Washington and Lee Law Review***.

Westin, A. F. 1997. Privacy and American business study. ***http://shell.idt.it/pab/women.html***.

Witmer, D., & Katzman, S. 1997. Online Smiles:Does Gender Make a Difference in the Use of Graphic Accents? ***Journal of Computer Mediated Communication***, [online].

World Economic Forum. 2011. ***Personal Data: The Emergence of a New Asset Class***. Available from https://www.weforum.org/reports/personal-data-emergence-new-asset-class.

Xu, H., Dinev, T., Smith, J., & Hart, P. 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. ***Journal of the Association for Information Systems***, 12(12): 798–824.

Xu, H., & Gupta, S. 2009. The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. ***Electronic Markets***.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. 2012. Measuring Mobile Users' Concerns for Information Privacy. ***ICIS***, (Ftc 2009): 1–16.

Yadav, S. 2010. Privacy on social networks a concern for old, not young. ***VentureBeat-Social***. http://venturebeat.com/2010/11/11/forrester-privacy-concerns-faceboo/.

Zawieska, K., Duffy, B., & Sprońska, A. 2012. Understanding anthropomorphisation in social robotics. ***Pomiary, Automatyka, Robotyka***.

Zukowski, T., & Brown, I. 2007. Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns. ***Proceedings of The 2007 Annual Research Conference of the South African Institue of Computer Scientists and Information Technologists on IT Research in Developing Countries***, 197–204. ACM.