Customer Surveillance:
Consumer Attitudes and Management Strategies

by

Kirk Anton Plangger

M.B.A., Simon Fraser University, 2010
B.A., University of Western Ontario, 2005

Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of
Doctor of Philosophy

in the
Segal Graduate School
Beedie School of Business

SIMON FRASER UNIVERSITY

Summer 2015

Approval

Name: **Kirk Anton Plangger**

Degree: **Doctor of Philosophy**

Title: ***Customer Surveillance: Consumer Attitudes and Management Strategies***

Examining Committee: **Chair:** Dr. Mark Wexler
Professor

Dr. Leyland Pitt
Senior Supervisor
Professor

Dr. Michael Parent
Supervisor
Professor

Dr. Richard Watson
Supervisor
Professor
Terry College of Business
University of Georgia

Dr. Christina Atanasova
Internal Examiner
Associate Professor

Dr. Tek Thongpapanl
External Examiner
Associate Professor
Goodman School of Business
Brock University

Date Defended/Approved: August 10, 2015

Ethics Statement

The author, whose name appears on the title page of this work, has obtained, for the research described in this work, either:

a. human research ethics approval from the Simon Fraser University Office of Research Ethics,

or

b. advance approval of the animal care protocol from the University Animal Care Committee of Simon Fraser University;

or has conducted the research

c. as a co-investigator, collaborator or research assistant in a research project approved in advance,

or

d. as a member of a course approved in advance for minimal risk human research, by the Office of Research Ethics.

A copy of the approval letter has been filed at the Theses Office of the University Library at the time of submission of this thesis or project.

The original application for approval and letter of approval are filed with the relevant offices. Inquiries may be directed to those authorities.

Simon Fraser University Library
Burnaby, British Columbia, Canada

update Spring 2010

Abstract

Due to technological advances, customer surveillance (i.e., the collection, capture, use, or storage of customers' personal data) is becoming less expensive and more covert. Brands use these personal data that contain needs, preferences, characteristics, behavior, attitudes, or other customer attributes (i.e., market intelligence) to develop more competitive products and services. Customer surveillance also can put stress on customer relationships with brands, thus brands must conduct customer surveillance in a way that is sensitive to customers' concerns. This dissertation investigates these concerns and proposes attitudes towards customer surveillance based on consumer privacy and value concerns. These attitudes explain differences in both cognitive and automatic reactions to customer surveillance, thus advancing the literature beyond the privacy calculus concept. Through 26 semi-structured interviews, this dissertation explores the implications of individuals having different levels of consumer privacy and value concerns. Next, it focuses on strategies to more efficiently and effectively conduct customer surveillance activities. It does this by proposing the surveillance prompt framework and a method of critically assessing the customer insight value of customer data sources. Using the responses of 1433 participants, four experiments show how different customer data factors predict customer insights (e.g., personality, future purchase behavior) with varying degrees of accuracy and consistency. The dissertation concludes with a summary of the contributions and implications of this research and calls for future customer surveillance research.

Keywords: Customer Surveillance; Market Intelligence; Consumer Privacy Concern; Value Concern; Surveillance Prompts; Customer Insights; Customer Data

Acknowledgements

There are many people I would like to thank that helped me through my PhD education and this dissertation, including the 26 interview informants and thousands of survey participants that gave up their valuable time.

I would like to acknowledge the outstanding support and encouragement of my senior supervisor, Leyland, who has guided me through fantastic, life-changing experiences over the past few years including hunting lions with cameras, finding a job in a place worth visiting, an open-heart surgery, culinary feats in North Vancouver (e.g., carrot "air"), many bottles of amazing wine, winning CTP grants, and publishing a few papers. I would also like thank Michael, my MBA and PhD supervisor, for his exceptional support and encouragement, but most of all, his frank comments that kept me honest and on track throughout my time at SFU. Thank you Rick, my PhD supervisor from University of Georgia, for your insights, theorizing sessions in London, and also for helping guide me through designing and writing the second paper.

We have a fabulous research community at Beedie that supports its PhD students in many ways. I couldn't have done it without the help and friendship of Joanne who still has time to help me through the best and the worst of last five years, even though she is running the whole program and also pursuing her fashion design dreams. I can't really say enough about the Beedie faculty, especially the Wine O'clock crew: Jan, Ian, Dave, Mila, Christina, and Danny. My PhD colleagues, co-authors, and friends – Adam, Karen, Anjali, Colin, and Anthony – have shared tones including two windowless offices, sleeping in airports, and "research" trips around the world (remember not to ask for ketchup in Austria, or to be crocodile when flying to Reykjavik the next morning).

I'd like to thank my colleagues for their constant inspiration in my new home at King's College London, especially Doug, Frauke, and the lunch crew. Last but not least, I would like to thank my family (Mom, Dad, Christa, and Eric) and my good friends (Tommy, Ed, Bernard, Jason, Nick, Alfred, Nathan, Michael, Johnny, and Paul) for their reassurance, support, love, and also for just keeping me sane these last five years.

Table of Contents

List of Tables

List of Figures

Chapter 1.

Introduction

Customer surveillance, or the collection, capture, storage, or use of customers' personal data (Lyon 2007), is an increasing concern because surveillance technologies have become less expensive and also more covert, efficient, and effective (Barnes 2006; Albrechtslund 2008; Bauman & Lyon 2013). From these customer data, brands gain market intelligence resources, or customer insights regarding the needs, preferences, characteristics, behavior, attitudes, and other customer attributes (Kohli & Jaworski 1990). Market intelligence has been shown to improve brand performance by aiding the competitiveness of a brand's products and services (McAffee & Brynjolfsson 2012; La Salle et al 2011; Puccinelli et al. 2011).

If customers' experience a threat to their personal privacy due a brand's activities (e.g., unauthorized data collection, selling personal data to third parties, data security breaches), customer surveillance may also put strain on customer relationships with that brand (Malhotra et al. 2004). Customers often develop intimate relationships with brands that are built on the trust that the brand will act with integrity in its interactions with customers (Fournier 1988; Morgan & Hunt 1994). If that trust is broken because of customer surveillance activities, customers may change their attitudes toward the offending brand and also their purchasing behavior (Andrejevic 2007; Turow 2008). Thus, brands need to manage their customer surveillance activities carefully to protect customer relationships.

Customers also face a trade off between protecting personal data and enjoying benefits from brands having access to their personal data (e.g., improved products, reduced costs, enhanced convenience). There has been much research on consumer privacy (see review Smith et al. 2011), including the privacy calculus concept that

explains cognitive decisions to disclosure personal data to brands (Culnan & Bies 2003). But the privacy calculus concept does not fully explain reactions that customers have to customer surveillance.

From a personal concern perspective (Baumgartner 2002) and recent psychological research regarding automatic behavioral effects (Kaheman 2011; Fitzsimmons et al. 2007), Chapter 2 investigates attitudes toward customer surveillance. These attitudes can theoretically explain the different automatic and cognitive responses that customers have to personal data requests depending on the relative magnitude of customers' consumer privacy (Malhotra et al. 2004) and value concerns (Aliawadi et al. 2001). There are four attitude archetypes (protectionists, capitalists, pragmatists, and apathists) that are examined using 26 semi-structured interviews. This chapter advances customer surveillance research beyond the cognitive privacy calculus concept (Culnan & Bies 2003) and explores the implications of customer surveillance practice.

Chapter 3 takes these implications further and examines methods of making customer surveillance more efficient and effective to narrow the scope of customer surveillance. It proposes a market intelligence framework that structures customer surveillance activities to answer basic prompts (when, where, what, how, who, why, and outcome). Using this framework, market intelligence resources would be more efficient by conducting customer surveillance that add to, not replicate, current data. Then, it proposes a method of evaluating customer insights by assessing the contribution to prediction accuracy and consistency of four data fit factors (data quantity, detail, content, and duality) in order to guide the choice of customer data sources. The chapter concludes with the results of four experiments testing this method and implications for customer surveillance researchers and managers.

The last chapter summarizes both the theoretical and empirical contributions of this research to the marketing, information systems, management, surveillance, psychology, and sociology literatures. The dissertation concludes with a call for future customer surveillance research.

Chapter 2.

Understanding Attitudes Toward Customer Surveillance

2.1. Introduction

As surveillance technology advances and becomes less expensive and more covert, individuals are increasingly concerned about their personal data privacy (Barnes 2006; Bennett 2008; Albrechtslund 2008). While some forms of surveillance can be valuable to the individuals under surveillance (e.g., a doctor monitoring a patients health) or can be important for public safety (e.g., police speed traps), other forms may be quite intrusive (e.g., government taps on telephone and email communication). Brands frequently conduct customer surveillance but customers react in different ways, as some are anxious about personal data privacy and others are not (Malhotra et al. 2004). Some brands attempt to diminish personal privacy costs by offering customers valuable tangible (e.g., monetary discounts) and intangible (e.g., product innovation) benefits. Building on the privacy costs (Culnan & Bies 2003; Lyon 2007) and value consciousness (Ailawadi et al 2001; Chandon et al. 2000) literatures, this paper seeks further understanding of how consumers experience customer surveillance.

Customer surveillance activities involve a brand's collection, capture, use, or storage of customers' personal data (Lyon 2007). More generally, surveillance involves "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (Lyon 2001: 14). Actors in surveillance activities can be described as *agents*, the person or organization conducting the surveillance, or *targets*, the person or organization under surveillance. Surveillance describes an agent's activity concerning a target's personal data, either with or without the target's knowledge, permission, or specifically identifying

the target (Lyon 2001; 2007). A target's personal data includes any aspect of the target including for example visual, financial, medical, habit, and location data. Surveillance involves both passive (i.e., target is unaware) and active (i.e., target is aware) collection of personal data. Targets have attitudes (i.e., thoughts, feelings, and intentions) towards agents collecting, using, or storing their personal data (Haggerty & Gazso 2002).

Brands perform customer surveillance to gain market intelligence, which includes needs, preferences, characteristics, behavior, attitudes, and other customer attributes (Kohli & Jaworski 1990). Brands analyze market intelligence to, for example, influence, target, and manage their customers, as well as proactively respond to customers' needs (Kohli & Jaworski 1990). Consider a general store in pioneer times in America's west, or a spice merchant in Renaissance Europe that often kept notes in ledgers or in the proprietor's mind on the purchasing and consumption behaviors of their customers. These written or mental notes ensured that the business was well stocked with the goods customers desired and sought products that fulfilled the needs of customers (Welch 2005). Due to customer insights derived from market intelligence collected by customer surveillance, brands can enjoy improved market competitiveness from enhanced customer loyalty, improved customer satisfaction, and stronger customer relationships (Jaworski & Kohli 1993). Thus, customer surveillance is a central aspect of marketing practice that enhances brand competitiveness.

From a relationship perspective, brands are primarily concerned with serving and satisfying current customers and attracting potential customers, not collecting personal data from customers (Berry & Linoff 2004; Fournier & Yao 1997). As customer relationships are built on customer perceptions of integrity and honesty (Marshall 1972; Fournier 1988), they may wither, and brand-switching behavior may occur, if customer surveillance activities threaten customers' personal data privacy (Lyon 2007; Morgan & Hunt 1994). In light of this, brands want to have enough data to be able to serve their customers, as well as remain competitive without threatening customer relationships by collecting too much personal data. Thus, brands need customer surveillance to remain competitive, but also must temper this need to protect customer relationships.

Customers also face a tradeoff between protecting their personal data and enjoying the benefits afforded by brands having access to their personal data (e.g., improved products, discounts, rewards). Although there is a growing literature on consumer privacy (see review Smith et al. 2011), little research has focused on the consumer's willingness to disclose personal data in return for valuable benefits. Instead the focus has been on other important topics, such as consumer privacy concerns (Malhotra et al 2004), or consumer privacy protection strategies (Ellison & Ellison 2009). One concept that does examine the consumer privacy cost-benefit tradeoff is privacy calculus, which investigates how consumers cognitively balance the benefits and costs of providing personal data (Culnan & Bies 2003). Privacy calculus has gained much interest in the literature (Dinev & Hart 2006; Kobsa 2007; Xu et al. 2011; Smith et al. 2011), but does not explain automatic personal data disclosure decisions.

Using Baumgartner's (2002) notion of personal concerns, specifically consumer privacy concern (Malhotra et al 2004; Smith et al 1996) and value concern (Chandon et al 2000), this research proposes attitudes towards customer surveillance that influence both cognitive and automatic decision-making regarding personal data disclosure. These attitudes explain consumers' varied reactions to customer surveillance activities, including for example changes in consumption frequency, brand switching behavior, relative indifference, and changes in attitudes towards the brand.

Section 2.2 reviews the literature on surveillance and proposes attitudes towards customer surveillance through eight theoretical propositions that define the consequences, influences, and composition, as well as archetypes of these attitudes. Section 2.3 discusses the mixed methods employed and their findings that add further depth to the understanding of these attitudes. Section 2.4 and 2.5 discuss and outline implications for both future academic and management research into customer surveillance. Section 2.6 offers a summary that highlights the main theoretical and empirical contributions.

2.2. Theory Development

This section begins with a brief examination of surveillance in general in order to understand its roots. Then, it defines customer surveillance and describes the various types of customer data, before developing a conceptual model based on eight theoretical propositions. The section ends with several research questions that guide the empirical investigations presented in section three.

2.2.1. Surveillance

Surveillance is pervasive in society and it touches some part of daily life for most individuals, whether they are aware of it or not (Lyon 2007; Andrejevic 2007). When conducting surveillance, agents may realize costs (e.g., operational costs of surveillance, relationships threats), and benefits (e.g., enhanced safety, improved competitiveness). Similarly, targets may realize costs (e.g., reduced in personal privacy, increased private data security risk), as well as tangible (e.g., advice, savings) and intangible (e.g., enhanced well-being, improve service) benefits (Turow 2008).

The agent's need for the target's personal data comes from a variety of sources, including for example curiosity, mistrust, security, safety, and competition (Shoemaker 1996). Acting as agents, many organizations frequently collect personal data from targets, but these organizations may be also under surveillance by the targets' own surveillance (Bauman & Lyon 2013; Lyon 2007). For example on one hand, national governments conduct surveillance on individuals and organizations both within and sometimes outside of their borders to protect national interests (e.g., national security, tax collection). On the other hand, these same individuals and organizations also conduct surveillance on the government through the popular press, various non-government organizations, lobby groups, and social media (Bauman & Lyon 2013; Bennett 2008; Shoemaker 1996). Surveillance actors – agents and targets – can be either individuals or organizations, and often have each other under some sort of surveillance.

Personal data privacy involves the ability of an individual to control the use, release, collection, storage, and access of personal data (Malhotra et al 2004; Solove

2008). The more private an individual, brand, or organization is, the more there is a desire for surveillance in others (Lyon 2007). For example on a micro scale, consider a committed relationship between two adults. If one person is very secretive or private, the other feels compelled to look closely at the first's actions. This might include examining bank statements or trying to find suspicious things (e.g., receipts or a strand of hair) in his or her personal places (e.g., car or wallet). On a macro scale, in a very private society where individuals can keep their personal activities hidden from public view (e.g., a bomb-making hobby, a machine-gun collection), there is a social need for surveillance when groups interact (e.g., work, festivals, public gatherings) to keep order so that citizens feel protected and safe from others that might threaten or hurt them. Brands desire consumers' personal data, which are hidden from them, to remain competitive, evaluate marketing strategies, and obtain consumer insights (Albrechtslund 2008; Turow 2008). While brands have an intrinsic need to engage in surveillance of their customers, the collection of these personal data also may breed mistrust among some consumers (Bennett 2008). Furthermore, brands have an obligation to secure customer data and prevent unauthorized access (Turow 2008, Andrejevic 2007). The target's desire for personal data privacy is linked to the agent's desire to conduct surveillance, which in turn threatens personal data privacy in a paradoxical fashion (Barnes 2006; Albrechtslund 2008).

Because of this link between data privacy and surveillance, the term surveillance often has a negative connotation related to the personal data privacy costs and security risks borne by the targets of surveillance despite the potential benefits that may accrue from surveillance (Albrechtslund 2008). Using health surveillance as an example, patients' personal data are collected by a wide variety of doctors, nurses, and other health practitioners to improve or maintain their health. Patients may experience costs in terms of privacy risks and negative emotions (e.g., embarrassment, discomfort, anxiety) due to the sensitive nature of the personal data, but these are often greatly outweighed by the health benefits. Similarly, the public's personal data privacy is infringed due to the Closed-Circuit Television (CCTV) recording of the public's activities in public spaces (e.g., streets, parks, inside buildings), but the public also benefits from enhanced personal security and safety because these recordings might deter criminal activity and promote a sense of public safety (Kietzmann & Angell 2010). While the term surveillance

might have an unfortunate negative connotation due to personal data privacy costs, valuable benefits do often accrue for surveillance targets.

In short, targets and agents of surveillance experience costs and benefits due to surveillance activity. The potential benefits of surveillance compel agents to seek out targets' personal data, thus potentially threatening those targets' personal data privacy. However, both agents and targets often enjoy valuable tangible and intangible benefits from surveillance activity. The next section describes a specific type of this activity, customer surveillance.

2.2.2. Customer Surveillance

Customer surveillance describes a brand's activities to collect, capture, use, or store customers' personal data (Lyon 2007). Customer surveillance adds to the body of market intelligence that a brand possesses, which has been shown to aid the competitiveness of a brand's products and services by developing customer insights (Kohli & Jaworski 1990). Market intelligence includes data on customers' needs, preferences, characteristics, behavior, attitudes, and other attributes (Kohil & Jaworski 1990).

Many brands have invested heavily in computerizing their data capture and processing infrastructures, thus making customer surveillance activities more powerful and less visible (Bauman & Lyon 2013; Turow, 2008). Since the 1980s, brands have set up large databases of customers' personal data, or customer relationship management (CRM) systems. These databases have become a central part of marketing operations for many brands across a wide variety of industries (Watson 2013).

There are five major types of customer data resources: basket, financial, spatial, journal, and network. Each data resource captures a different set of personal data from customers, as well as often utilizing different surveillance technologies (see Table 2.1). *Basket* data involve collecting the specific content of customers' purchases in a brand or a network of brands (e.g., loyalty programs) and are often collected nearly effortlessly at the point of sale. Similar to basket data, *financial* data capture the purchase value and often location when customers use credit cards, debit cards, or online payment services

(e.g., Pay Pal, Google wallet). *Spatial* data capture customers' physical location by using tracking technologies, such as for example Radio Frequency Identification (RFID), Bluetooth, a Global Positioning System (GPS), or Internet Protocol (IP) addresses. *Journal* data capture audio, video, or web-tracking records of customer behavior on the Internet, telephone, emails, and in person. *Network* data collect and capture customers' social interactions and activities by observing customers socializing with each other and can be collected using online social networking sites or using offline social networks, such as for example conferences, sports or hobby societies, and professional organizations. Together these five customer data resources describe the major types of data that are captured and collected by brands using various customer surveillance technologies. Customer surveillance results in a reduction of customer privacy, but they react different ways. The next section introduces attitudes towards customer surveillance that explains this varied reaction.

Table 2.1 Types of Customer Data Resources

Data Resource	Customer Data Collected	Examples of Customer Surveillance Methods
Basket	Detailed purchase data (restricted to a brand or a network of brands)	Grocery store cards, frequent flyer programs, loyalty programs
Financial	Basic purchase data (unrestricted)	Credit cards, debit cards, Pay Pal, Google Wallet
Spatial	Physical location data	GPS, RFID, Foursquare, OnStar, Yelp, credit cards, IP addresses
Journal	Video, audio, or digital record of behavior	In store CCTV cameras, telephone recording systems, DoubleClick, comScore, website cookies
Network	Events, pictures, online posting, Social networks, etc.	Facebook, Flickr, LinkedIn, Yelp, Foursquare, conferences, societies

2.2.3. Attitudes Toward Customer Surveillance

Attitudes toward customer surveillance are cognitive structures that exist outside of particular experiences that shape how individuals think, feel, and intend to behave towards customer surveillance. Individuals perceive customer surveillance both individually and sometimes collectively with others, especially through the mass media (McCombs 2004). But when perceptions are shared, individuals often have very different

reactions (Xu et al 2011) that can be explained by these attitudes. For example, in 2011, Apple experienced consumer outrage when it became known that it had installed a program in all mobile Apple products, including the popular iPhone and iPad, that stored specific location data of where that device had been. The brand faced public scrutiny over this action and was also investigated by several members of the US Congress. Consumers shared similar perceptions about this event (i.e., Apple was tracking customers' movements) because of mass media coverage, but had varied reactions. At the extreme, consumer groups brought lawsuits against Apple, which the company has successfully fought (Gayathri 2013). Some customers reacted by turning off the location tracking in the device's settings. Others may have switched brands in response to the tracking episode. But many customers took no action at all as is evident in the growing sales of the brand's devices.

Attitudes toward customer surveillance can explain these various reactions while holding perceptions as shared among consumers. Consider two consumers that share the same perception of a brand's surveillance activities, but they have different attitudes towards customer surveillance. The one that has a relatively more negative attitude toward customer surveillance is more likely to terminate the relationship with the brand that is conducting customer surveillance than the other consumer. While it is easier to see the difference in reactions when holding perceptions as shared, this likely also applies to cases where the consumers do not share the same perceptions of customer surveillance.

Attitudes are held with reference to some part of an individual's experience in reality (Ajzen & Fishbein 1977; Millar & Millar 1990). An attitude embodies a person's evaluation of an attitude object (e.g., tangible: a physical object, an animal, a person; intangible: an idea, a policy, a religion), which has cognitive, affective, and intended behavioral dimensions. The cognitive dimension includes the attributes of and beliefs about an attitude object. The affective dimension contains the emotions and feelings associated with an attitude object (Millar & Millar 1990). The intended behavior dimension includes planned behavior when physically or mentally encountering an attitude object (Azjen & Fishbein 1977). Thus, attitudes towards customer surveillance are proposed to have the following influences on an individual:

Proposition 1: Attitudes toward customer surveillance influence how consumers *feel* about a brand that conducts customer surveillance.

Proposition 2: Attitudes toward customer surveillance influence how consumers *think* about a brand that conducts customer surveillance.

Proposition 3: Attitudes toward customer surveillance influence how consumers *intend to behave* towards a brand that conducts customer surveillance.

While intended behavior is a dimension of an attitude, individuals do not always behave how they intend to behave (Azjen & Fishbein 1977; Millar & Millar 1990). For example, imagine an individual would like to lose a few pounds, and intends on eating healthy. But when faced with an offer of a free piece of chocolate cake, his resolve folds and pushes back his intention to diet until the next day. Thus, he broke his intention to eat healthily. Attitudes can show researchers and marketers how individuals intend to behave, but that intention does not guarantee actual behavior (Ajzen & Fishbein 1977).

While individuals' commitment to intentions explains part of this gulf between intended behavior and actual behavior (Ajzen & Fishbein 1977), the Theory of Planned Behavior (Ajzen 2011) describes how intentions capture the motivational factors (e.g., attitudes, subjective norms, etc.) that influence actual behavior. Moreover, there are non-motivational factors that influence actual behavior (e.g., time, money, skills, opportunity, perceived or actual behavioral control; Ajzen 2011). Thus, even though an individual intends some action due to motivational factors, there are other non-motivational factors that may upset the intended action. By understanding these non-motivational factors, a more accurate prediction of actual behavior can be produced. However, regardless of the accuracy of actual behavior prediction, attitudes toward customer surveillance are propose to have some effect on actual behavior. Thus,

Proposition 4: Attitudes toward customer surveillance influence how consumers *actually behave* towards a brand that conducts customer surveillance.

Attitudes form both cognitively through reasoned thought, and affectively through experienced emotions (e.g., needs, wishes, dreams, feelings, and other emotional factors). Motivational pressures may be associated with the relative contribution of the cognitive and affective elements that for an attitude (Edwards 1990; Kim, Lim & Bhargava 1998). For example, the cognitive element may be dominant when an attitude helps explain the wider environment or test reality (Edwards 1990). The affective element may be dominant when, for example, an attitude provides some measure of gratification, or protects against threats to self-image (Edwards 1990; Kim et al 1998). Moreover, attitudes can form with and without conscious thought or consideration (Janiszewski, 1988), therefore individuals may not fully understand how their attitudes have formed. Attitudes toward customer surveillance are proposed to form using cognitive and affective elements of past experience with customer surveillance:

Proposition 5: Attitudes toward customer surveillance are formed through cognitive experiences with customer surveillance.

Proposition 6: Attitudes toward customer surveillance are formed through affective experiences with customer surveillance.

In sum, attitudes toward customer surveillance have influence over how individuals think, feel, intend to behave, and actually behave towards a brand that conducts customer surveillance. These attitudes help explain the varied reactions of consumers when perceiving customer surveillance activities and may be formed using both cognitive and affective elements of past experience.

2.2.4. Beyond Privacy Calculus

Culnan and Bies (2003) introduce the notion of privacy calculus where consumers balance the benefits and costs of disclosing personal data to a brand. These authors claim that consumers critically weigh the pros and cons each time they encounter a personal data disclosure request in what is termed the second exchange (Glazer 1991). The first exchange is the exchange of goods or services for money or resources (Bagozzi 1975). If the benefits outweigh the costs, consumers decide to disclose the data requested, and do not disclose if the costs outweigh the benefits. The

privacy calculus approach has been popularly adopted by information systems scholars in varied empirical settings, including e-commerce transactions (Dinev & Hart 2006), personalized websites (Kobsa 2007), and location-based services (Xu et al. 2009).

However, recent theoretical developments (Kahneman 2011; Dane & Pratt 2007) and empirical evidence (Hassin et al. 2009; Fitzsimmons et al. 2008) on non-conscious decision-making reports that consumers rarely make calculated decisions and often make automatic choices. These automatic choices could be influenced by many things, including heuristics (Hoyer & Brown 1990), habits (Aarts & Dijksterhuis 2000), past-purchase behavior (Aarts et al. 1998), and attitudes towards aspects of the decision (Woodside & Trappey 1992). Thus, in the second exchange, other factors may have greater influence than a cognitive privacy calculus process. Attitudes toward customer surveillance influence how consumers both automatically and cognitively react to customer surveillance. Like privacy calculus, these attitudes are theoretically based on two personal concern dimensions associated with the costs and benefits of the second exchange. As attitudes, their influence on consumers' decision-making are wider than the cognitive calculation suggested by the privacy calculus concept.

Attitudes toward customer surveillance consist of two theoretical dimensions of personal concern: consumer privacy concern and value concern. Personal concerns are "the goals that people pursue in their lives and the effects that these goals have on personal outcomes" (Baumgartner 2002: 287). *Consumer privacy concern* involves a consumer's level of anxiety about the potential personal privacy costs associated with consumption. *Value concern* involves a consumer's motivation to seek additional benefits and reduced costs that accrue from consumption. The relationship between these two personal concerns forms attitudes toward customer surveillance that cognitively and automatically influence decisions to disclose personal data depending on the relative magnitude of each concern. Thus,

Proposition 7: Consumer privacy concern is a dimension of attitudes towards customer surveillance.

Proposition 8: Value concern is a dimension of attitudes towards customer surveillance.

Consumer Privacy Concern

Consumer privacy concern is the level of concern a consumer has over his or her private personal data in the context of consumption (Smith et al 2011). Customer surveillance rarely provokes a consumers' sense of privacy. In cases where it does, it is often due to some brand error or misuse of personal data, which is sometimes brought to consumers' attention by news stories in the mass media (Lyon 2007). Consumers do not always see the personal data collected by brands as private. In the following paragraphs, privacy is examined through various definitions, as well as two characteristics of personal data disclosure: data centricity and relationship intimacy. Then, consumer privacy concern is discussed with special attention to the three elements of surveillance activity: collection, control, and consumer awareness.

Privacy is an outcome of a person's desire to withhold certain personal data from others (Larson & Bell 1988). As a general legal concept, privacy has lost a precise definition since it means different things depending on context (Solove 2008). Privacy is an umbrella term that refers to a wide group of conceptions, such as for example: intimacy (Inness 1992), personhood (Craven 1976), secrecy (Posner 1981), shame (Schneider 1972), limited access to self (Godkin 1880), the right to be left alone (Warren & Brandeis 1890), and control over personal data (Westin 1967). Westin (1967) provides a useful and bounded definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent data about them is communicated to others" (7). Privacy also provides self-definition by outlining the boundaries of an individual's self-concept and provides emotional release when private personal data are shared, which defines the context for data to be perceived as private (Larson and Bell 1988; Smith et al 2011). Individuals perceive personal data as private when that data are central (e.g., birth date, sexual orientation, relationship status, address, credit card, and health data) to their identity or the relationship between the individual and the data recipient is not intimate (Marshall 1972).

Consumers may have intimate relationships with the brands they interact with on a regular basis (Fournier 1988). Consumers may feel that the personal data they provide to brands is not private due to the nature of their relationship with the brand and the perceived non-centrality of the data requested. For example, Apple requests credit card

data to use the brand's iTunes service even before a consumer chooses to purchase a song, book, or movie. Credit card data are arguably considered quite central personal data due to the risks associated with identity theft and financial security. Consumers that provide this personal data must feel that their relationship with Apple is intimate enough to provide this personal data to the brand. Yet, regardless whether a specific piece of personal data are deemed as private or not in a certain context, an individual's level of consumer privacy concern remains the constant in the short-term, although other consumers may have different levels of concern.

Consumers and brands exist in society where a social contract between them exists. Social Contract Theory describes individuals' obligations to each other under an agreement to form the society where they live, and has its origins in Socrates' *Crito* and Plato's *Republic*. Using Social Contract Theory, scholars have provided insight into the brand-consumer relationship (Donaldson & Dunfee 1999) and the personal data exchange between brands and consumers (Culnan & Bies 2003). Consumer privacy concern involves an individual's anxiety that brands will not be faithful to the social contract between them. These privacy concerns can be broken down into three elements of surveillance activity: collection, control, and consumer awareness (Malhotra et al 2004).

Collection is the operational component of customer surveillance, which is how a brand obtains a consumer's personal data (e.g., surveys, cameras, loyalty cards, location-tracking devices, consumer data purchases; Malhotra et al 2004; Smith et al 1996). Consumers may employ customer secrecy strategies to hide their personal data, such as for example an obfuscation strategy or the intentional provision of misinformation (Ellison & Ellison 2009; Plangger & Watson 2015). The anxiety over personal data collection is an important contributing element to a consumer's consumer privacy concern (Malhotra et al 2004; Smith et al 1996).

Control reflects consumers' ability to actively control the kinds of personal data collected, as well as the usage, storage methods, and security measures employed by the brand (Malhotra et al 2004). Control can be seen when consumers approve, opt-in or out of, or modify customer surveillance activities. The anxiety regarding the lack of

control over collection, use, and storage of personal data, as well as the security of disclosed data, is an important element of consumer privacy concern (Malhotra et al 2004).

The lack of *consumer awareness* of customer surveillance activities and surveillance creep is an important contributor to consumer privacy concern (Culnan 1995; Malhotra et al. 2004). This passive anxiety is highly correlated to the more active control component, but distinct as awareness reflects the specificity of the personal data collected and the transparency of the data collection process. Consumers often disclose personal data freely (e.g., loyalty cards), but they might forget or not realize disclosure is occurring in a specific situation or environment. Surveillance creep is the use of disclosed personal data over and above the primary purpose agreed to (Culnan 1993; Lyon 2007). For example, consumers would be concerned if a loyalty program sold identifiable data to a health insurance company to check on these consumers' consumption choices. Whether regarding the instance or the scope of customer surveillance activities, anxiety over awareness is an important element of consumer privacy concern.

Collection, control, and consumer awareness are the key elements of surveillance activity that form consumer privacy concerns. These concerns have been measured using questions about consumers' anxiety over the various components of surveillance (Malhotra et al. 2004; Smith et al. 1996).

Value Concern

Value concern is the level of personal concern a consumer has over seeking out personal benefits and reduced costs. The value-concerned consumer has been researched in the past (Aliawadi et al 2001; Lee & Ariely 2006; Yoon & Vargas 2010), however, this type of consumer has often been narrowly defined as deal-proneness, or seeking out monetary discounts and other marketing promotions (Litchenstein et al 1995). While deal-proneness is related to value concern, value concern describes consumers' broader propensity to actively seek increased benefits (e.g., discounts, coupons, sales, points) and reduced costs (e.g., decreased financial, convenience, or

other costs). In essence, value concern is a consumer's goal to gain additional and higher quality resources at a lower personal cost.

From a marketing promotion perspective, consumers have varying degrees of value concern (Ailawadi et al. 2001). There are three utilitarian (i.e. extrinsic) and three hedonic (i.e. intrinsic) benefits can accrue from a consumption decision (Chandon et al 2000). The utilitarian benefits include monetary savings or discounts (Blattberg & Neslin 1990), quality increases (Holbrook 1994), and convenience (Hoyer 1984). The hedonic benefits include value expression (display morals or ethics; Holbrook 1994), exploration (stimulation and variety; Baumgartner & Steenkamp 1996), and entertainment (amusement and aesthetics; Holbrook 1994). The marketing literature understands many aspects of the benefits of value concern when it comes to sales promotions, but outside of this specific, albeit a large and important subject, there has been little research.

Privacy researchers have largely discounted the benefits of customer surveillance as being relatively small compared to the personal privacy and data security costs that are borne by consumers (Culnan & Bies 2003; Turow 2008; Bennett 2008). However, this paper contends that the personal concern for value stretches to the decision to disclose personal data. Consumers vary on their personal concern for value, much like they vary in consumer privacy concern. When consumers are highly concerned with value, they are more likely to disclose personal data provided valuable benefits are offered. Therefore, value concern is an integral dimension of attitudes toward customer surveillance.

2.2.5. Conceptual Model

In sum, the theory development section introduces attitudes toward customer surveillance to explain the cognitive and automatic reactions of consumers when confronted with customer surveillance activities (see Figure 2.1 for the conceptual model). These reactions are manifested in feelings, thoughts, as well as intended and actual behaviors towards a brand that conducts customer surveillance. These attitudes

have consumer privacy concern and value concern dimensions, as well as being formed by past cognitive and affective experiences with customer surveillance (see Table 2.2).

Figure 2.1 The Attitude Towards Customer Surveillance

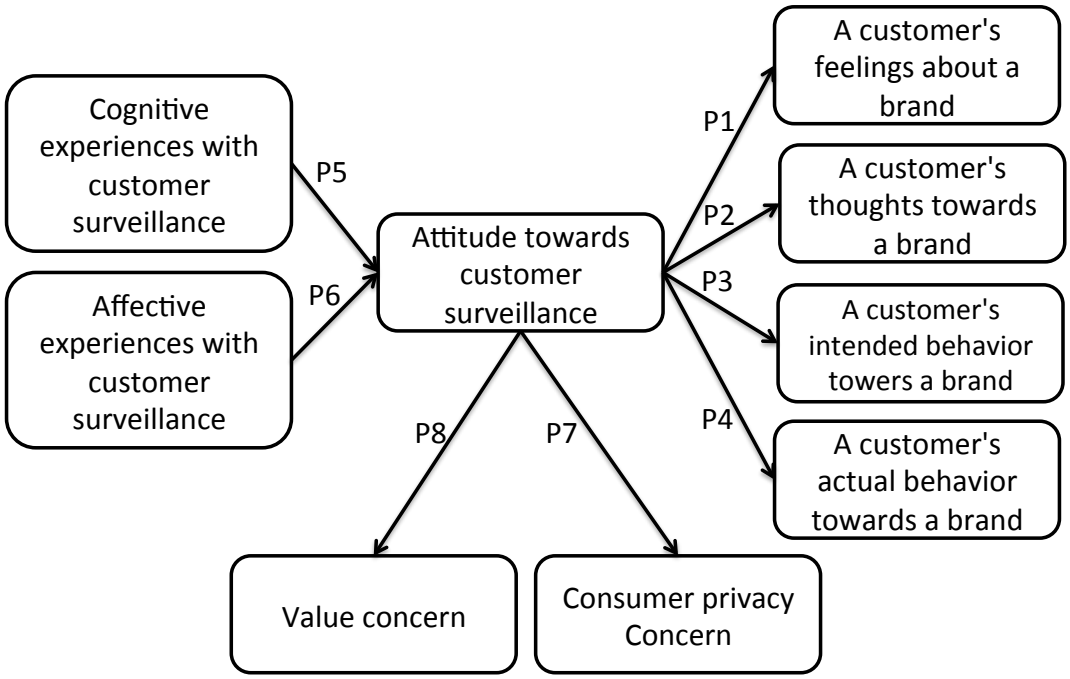


Table 2.2 Theoretical Propositions

Number	Propositions
P1	Attitudes toward customer surveillance influence how consumers *feel* about a brand that conducts customer surveillance.
P2	Attitudes toward customer surveillance influence how consumers *think* about a brand that conducts customer surveillance.
P3	Attitudes toward customer surveillance influence how consumers *intend to behave* towards a brand that conducts customer surveillance.
P4	Attitudes toward customer surveillance influence how consumers *actually behave* towards a brand that conducts customer surveillance.
P5	Attitudes toward customer surveillance are formed through cognitive experiences with customer surveillance.
P6	Attitudes toward customer surveillance are formed through affective experiences with customer surveillance.
P7	Consumer privacy concern is a dimension of attitudes toward customer surveillance.
P8	Value concern is a dimension of attitudes toward customer surveillance.

Since individuals have different magnitudes of personal concern for consumer privacy (Malhotra et al, 2004) and value (Ailawadi et al. 2001), there are four archetypical attitudes towards customer surveillance (see Figure 2.2). On one extreme, *protectionists* are highly concerned with consumer privacy but are not concerned with value, so they are likely to automatically refuse personal data requests even when offered valuable benefits. On the other extreme, *capitalists* are very concerned with seeking out value without much concern over their consumer privacy, so they are more likely to automatically provide personal data if there is a clear benefit to them. In between, *pragmatists* have high personal concerns for both consumer privacy and value, so they are more likely to cognitively consider personal data requests. Lastly, *apathists* do not consider either consumer privacy or value to be a personal concern, so they are more likely to be influenced by other factors of a personal data request. These archetypes can theoretically explain the varied reactions to customer surveillance, but there are a number of research questions that seek further understanding and clarification (see Table 2.3). These research questions are empirically explored in the next section.

Figure 2.2 Archetypes of Attitudes towards Customer Surveillance

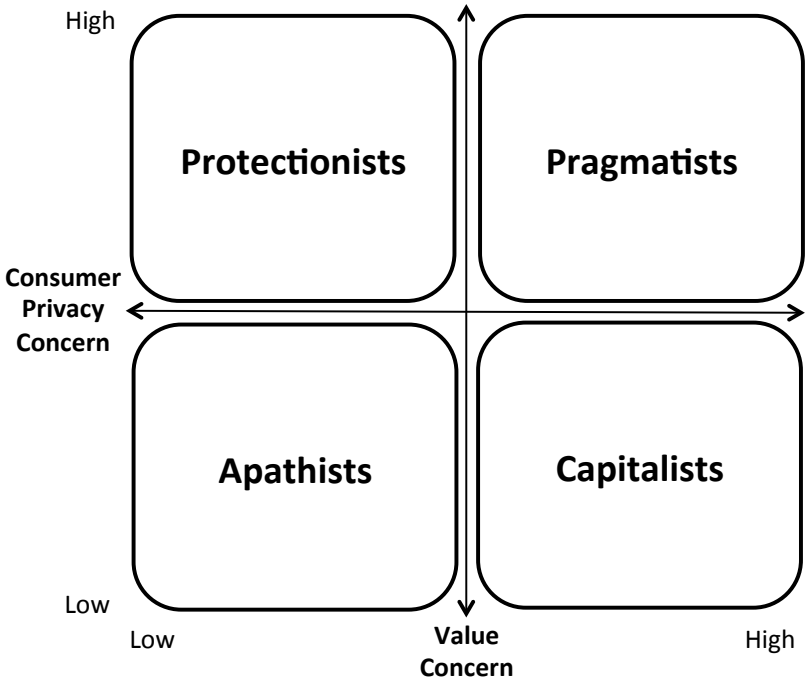


Table 2.3 Research Questions

Number	Question Description
1	How do consumers define privacy?
2	How do consumers define personal data?
3	What obfuscation strategies are used?
4	Why do consumers use these obfuscation strategies?
5	How do consumer privacy concerns influence consumers' willingness to provide personal data to brands?
6	How do value concerns influence consumers' willingness to provide personal data to brands?
7	How do consumer privacy and value concerns shape attitudes towards customer surveillance?
8	To what extent is the decision by consumers to disclose personal data to a brand made automatically?
9	What are the managerial implications of attitudes towards customer surveillance?

2.3. Empirical Investigations

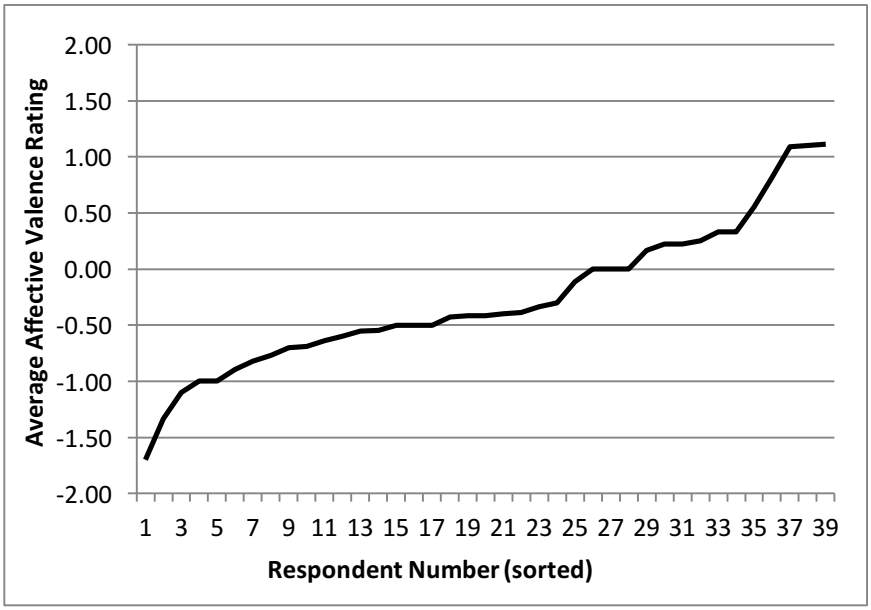
This section reports a mixed method investigation to answer the nine research questions. From the results from a preliminary survey, a qualitative semi-structured interview study was designed and then conducted using 26 informants. During analysis, informants have been placed in one of the four archetypes of attitudes toward customer surveillance based on their apparent level of concern for consumer privacy and value. The results are then compared and contrasted to explore each archetype in detail and provide insight into the research questions.

2.3.1. Preliminary Survey

This study provides evidence that attitudes towards customer surveillance do indeed vary. Maio & Haddock (2009: 29-30) outline a simple survey-based method that explores how consumers think, feel, and behave towards something. This method is an

explicit form of attitude measurement that uses self-evaluations about respondents' thoughts, feelings, and behaviors about personal data collection by brands. Prior to a lecture, 39 MBA students at Simon Fraser University participated in the survey, which involved a set of open-ended questions that attempted to measure all three attitudinal elements (Maio & Haddock 2009). Respondents completed three partial sentences (i.e., Firms that collect customer information are…, Firms that collect customer information make me feel…, I react to firms collecting customer information by…) with as many adjectives as possible. Respondents then asked to rate these adjectives on a +2 (very positive) to -2 scale (very negative). This produced a set of affective ratings on respondents' adjectives that were then averaged for each respondent (see Figure 2.3). The affective ratings have a mean of -0.27 and a standard deviation of 0.66.

Figure 2.3 Average Affective Valence Rating

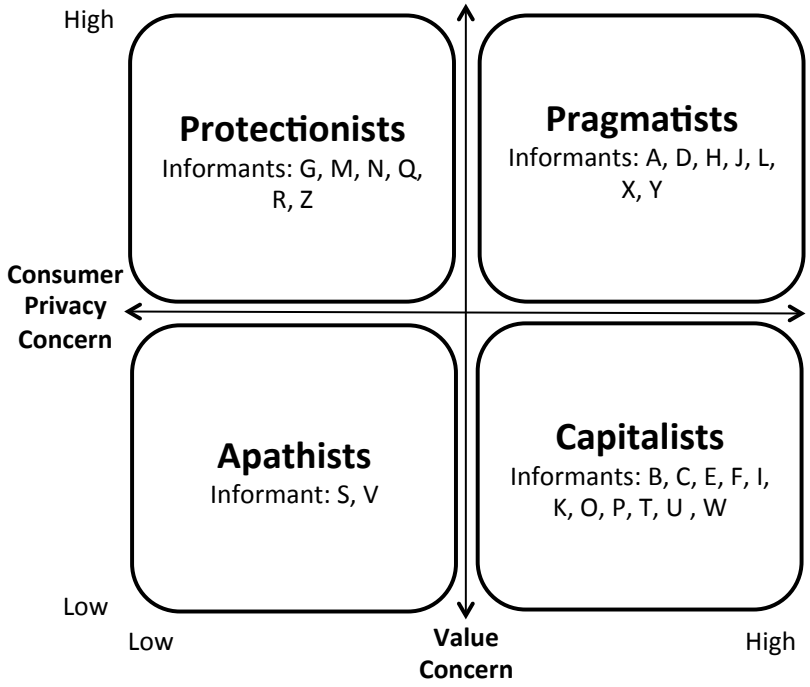


Even in a relatively small sample of similar individuals (i.e., MBA students), there is considerable variation between respondents with regard to the magnitude and valence of the average affective ratings. This survey shows exploratory evidence that attitudes toward customer surveillance do vary. But, this survey does not inform the drivers of this variation, explore the implications of having a positive or negative attitude, or consider consumer privacy and value concerns. The following interview study provides additional insight into these topics.

2.3.2. Interview Study

Twenty-six depth consumer interviews investigate how informants experience customer surveillance by examining their reported consumer privacy and value concerns. The results indicate that informants have various levels of consumer privacy and value concern, and also that for some informants the decision to disclose personal data is often a quick, automatic decision rather than a calculated decision. The interviews reported below examine informants' attitudes towards customer surveillance through discussing consumer privacy concerns, consumer value concerns, and the approach that they take when encountering customer surveillance. Informants fall into all four archetypes of the attitude towards customer surveillance (protectionists, capitalists, pragmatists, and apatheists; see Figure 2.4). The following sub-sections describe the interview method employed, informant details, and then report the findings.

Figure 2.4 Informant Attitudes Toward Customer Surveillance



Interview Method

Interview and other qualitative methods offer deep explanations of phenomena in the effort to understand specific aspects of individual experience (Cresswell 2009;

Arnould et al 2006). Thus, interviews are an appropriate empirical method as the study explores consumer attitudes toward customer surveillance, an unresearched attitude, from the perspective of the personal concerns of consumer privacy and value. Semi-structured interviews offer deep examination into an informant's responses, while still retaining some structure to compare experiences across informants (Creswell 2009). Thus, this study uses semi-structured informant interviews to understand both the perceived personal data privacy costs, as well as hedonic and utilitarian benefits experienced by consumers in the context of customer surveillance.

A wide sample of initial informants is selected to participate in interviews across various demographic categories (e.g., gender, age, cultural, and occupation) to bring a broad range of perspectives on customer surveillance, consumer privacy, and value concern. These informants were asked to suggest other potential informants using a snowball sampling method (Creswell 2009). Interviews were collected until theoretical saturation had been reached, or no new insights emerged from the informants' responses (Gillham 2005; Creswell 2009).

All interviews conducted were semi-structured using an interview worksheet developed using the theoretical propositions above with the intention to direct informants to a selection of customer surveillance topics, but also at the same time, allow for flexibility in informants' responses. Informants were asked to first define the concepts of privacy and personal data. Next, the interviewer probed deeper into informants' views on and experiences with customer surveillance in general (e.g., discuss the point/loyalty cards in your wallet), without using the term 'customer surveillance'. Then, informants reported specific positive and negative experiences with personal data requests to examine their feelings and thoughts, as well as their intended and actual behavior towards customer surveillance. The interviewer often probed for a detailed description and analysis of the benefits and costs that were realized by those experiences. Next, informants advised a close friend on how to go about responding to personal data requests. Then, informants advised brands on how to form policies concerning the collection and handling of personal data. Lastly, some demographic data are recorded to aid informant comparison.

Recordings and interviewer notes of each interview have been collected digitally for transcription. These data were analyzed using an inductive approach (Glasser & Strauss 1967; Arnould & Fischer 1994) that allowed insights to emerge from individual transcripts and comparative analyses of many transcripts. This approach involved (1) the open coding of the first set of ten interviews; (2) developing general themes and patterns that emerge from the analysis to create core categories; (3) axial coding (i.e., the disaggregation of core categories) to refine the definition of and understand the relationship between core; and (4) hermeneutic interpretation of the findings (Arnould & Fischer 1994). Each informant was placed into one of the four attitude archetypes after transcripts were reanalyzed in terms of the evident consumer privacy and value concerns (see Figure 2.4 above). Although discussions with several consumer privacy experts about coding assessments and theme conclusions was done to minimize the effects of the single coder, there is possibility of a single researcher coding bias.

Informant Details

Theoretical saturation became evident after 22 interviewers, however a further four additional interviews were performed as they were already scheduled and planned. Thus, 26 interviews were conducted (see Table 2.4 for informant details) with an average length of approximately 24 minutes and a total of approximately 9 hours 44 minutes. There was a mix of genders with 14 informants being female and 12 being male. The average age of informants was 34 years old, with a wide age range from the early twenties to the early fifties. Informants came from a variety of industries and professions, and no one category dominated. In terms of nationality, Canadians made up the biggest of the sample with 13 informants, however to add an element of generalizability, other nationalities were sought out to balance the empirical focus on Canada, including British, American, Chinese, Taiwanese, Australian, Saudi Arabian, Turkish, German, Korean, and South African informants.

Table 2.4 Informant Details

Informant	Gender	Age	Industry	Nationality
A	Female	Early 30s	Student	Canadian
B	Male	Early 30s	Student	Canadian
C	Male	Late 40s	Finance	British
D	Male	Early 40s	Administration	British
E	Female	Early 30s	Finance	Canadian
F	Female	Late 20s	Construction	Canadian
G	Female	Early 50s	Sales	Canadian
H	Male	Late 20s	Law	Australian
I	Male	Mid 30s	Education	Taiwanese
J	Female	Early 30s	Healthcare	Canadian
K	Female	Late 20s	Education	South African
L	Female	Mid 30s	Creative	Canadian
M	Female	Mid 30s	Education	American
N	Female	Early 30s	Healthcare	Canadian
O	Male	Early 30s	Education	Canadian
P	Male	Mid 20s	Finance	Chinese
Q	Female	Early 20s	Student	American
R	Male	Late 20s	Healthcare	Canadian
S	Male	Mid 30s	Creative	Canadian
T	Female	Late 30s	Administration	Canadian
U	Male	Early 40s	Student	Canadian
V	Male	Late 20s	Student	Chinese
W	Female	Mid 30s	Education	Saudi Arabia
X	Female	Early 30s	Student	Germany
Y	Female	Early 30s	Consulting	Korean
Z	Male	Early 30s	Education	Turkey

Informants' Privacy and Personal Data Definitions

All the informants roughly define privacy in same way. For example, Informant H provides this definition: "Privacy is a right to your own personal information, right to control it. Yeah, right to possess and control or dictate the terms on which someone else cannot control or possess or use the information". Similarly, Informant M said,

> …privacy to me is the right to not share everything about myself with the general public and perhaps a little bit of control over who gets to know specific facts about me that may not be obvious to an average person. (Informant M)

In both of these examples, privacy is seen as both the choice not to disclose certain personal data, and moreover privacy is also the ability to control the use of disclosed data.

However, personal data varied in the exact definition across informants. In some cases informants only identified very basic data about their person, such as in Informant I's case, where he said in response to a question about the kind of data he finds personal,

> Your phone number, your address, and your birthdate, sometimes even your gender. It depends on the context, yeah but mostly it will be your date of birth, yeah. (Informant I)

Other informants included many other forms of personal data, such as Informant G who said that personal data included

> Your age, your phone number, your social-insurance number, your credit card numbers, your address, almost anything that could identify you as a person. (Informant G)

Still others defined personal data as data that is identifying and that by combining various pieces of data that might be more general in nature, the combined data becomes personal. For example, Informant E reported, that personal data was

> Anything that would distinguish me from another person. So I don't think my birthday [alone] is personal because a lot of people share my birthday, but maybe my birthday in combination with my name because it becomes personal or with my address becomes personal because it is a way of identifying me. Yeah, anything that would separate me from another person I think is personal. (Informant E)

These definitions in all cases shaped and colored the resulting discussions about the reasons why brands collect customer data.

Informants' Theories and Actions

The informants' theories concerning why brands collect their personal data were fairly consistent across informants. For example, Informant A theorized,

> [Brands] probably want to know where I live so they know where their consumers are coming from. There are a lot of [brand's name]. It's a chain. So they probably want to know where their customers are shopping from, or where they live. (Informant A)

Similarly, Informant C thought that "because someone who has bought from them once is more likely to buy it again." Along the same lines, Informant A theorizes brands' motivations when she said, "I think that they are collecting data in order to target me as a consumer, so that they can get ore money out of me." Informant T echoes this by stating,

> I like to believe, and maybe this is naïve, but I like to believe that it is like they are going to get a better understanding of their customers so they can service their customers better and what their customers need. (Informant T)

Thus, regardless of the positive or negative valence of the theory, all informants recognized that brands that collect customer data are doing so to further their efforts to market to and serve their customers.

Seemingly regardless of the magnitude of privacy or value concern, ten informants reported that they use obfuscation strategies (i.e., purposefully providing wrong or confusing data) when dealing with some brands. The reason for this strategy was mostly due to irritation or annoyance, as Informant E said,

> I really don't like giving out my email because I really hate it. I never ever read the emails that [brands] send me. So, often I have fake email accounts that I give. Like I have a Hotmail account that I can't even log into anymore and I just give that one out and then I really don't have to worry about it. (Informant E)

Informant A reported a similar strategy to avoid irritation,

> When people ask for my email address and telephone number for like memberships, club cards whatever, I always give them fake email and fake telephone numbers. (Informant A)

Other informants have different strategies to avoid irritation, such as Informant L who reported,

> So I took the card but I was supposed to fill out the form, right, and return it, but I never did it. So I kept the point card but they have no idea of who the card belongs to but I can still use the points. I collect them. (Informant L)

Thus, many informants seem to try to avoid irritation and annoyance from brands contacting them by providing false or confusing data.

Exploring the Attitude Archetypes

These different attitude archetypes depend on the magnitude of informants' consumer privacy and value concerns. Each archetype is separately described in the following sub-sections using transcription evidence. Although some informants did exhibit high degrees of privacy concern when they discussed general or government surveillance, this did not always translate into a similar level of consumer privacy concern. Please note, this analysis only examined surveillance with regards to customer surveillance and brands collecting data from customers.

Protectionists

Protectionist informants exhibit a high consumer privacy concern and a relatively low value concern. Turning first to consumer privacy concerns, Informant N highlights collection and awareness concerns in her comment,

> You know I wouldn't feel good about if [brands] kind of knew all sorts of stuff about me, and I wasn't aware of it and I didn't actually supply it to them… I wouldn't like it if they have all my info and they knew everything about me before I step through the door. (Informant N)

Similarly, Informant G displays considerable concern over private data collection when she states, "it's nobody else's business unless I decide it is somebody else's business".

When discussing reading corporate privacy policies, Informant G gives insight into how strongly she feels about consumer privacy protection,

> If they can give your data out to another source, or another company, or it is going to be used for marketing purposes, as soon as I hear that they can use it for marketing purposes, I would never give out that data. (Informant G)

Both of these informants present their acute anxiety that their personal data are at risk when disclosing data to brands.

Informant R is also careful about who he provides his personal data to as when he advised a hypothetical close friend, he said,

> Maybe ask more questions you know if a company is asking you questions… ask them why they need to know that. You know, so you don't just share your information because someone asked you to. Try to find out why that group or that company wants to know that information. So in general, just be careful. I guess that's the biggest thing here. (Informant R)

Informant R goes on to confirm that he is skeptical of brands' intentions regarding his personal data. In his case, as in many other protectionists, his concern for privacy stretches to his professional and social life, not just his consumer activities.

Informant N also confirms her feelings towards collection of private data by stating that, "Yeah because it is almost sneaky you know like they have the advantage and then it makes it hard to say no if you didn't really want it." She feels she would not be able to resist the marketing efforts of brands that would have access to her private data, and thus justifies her refusal to disclose her personal data.

In fact, many protectionist informants claim that there are few benefits that accrue from customer surveillance that they care about. For example, in response to a direct question of what benefits she received for providing personal data to brands, Informant G reported,

> For me? Zero, zero benefits for me. For them, there is, to acquire [my personal data] because they can use it for marketing. But for me it is a

> liability for me. People can break in and use your personal information, or unsavory things too. (Informant G)

It is clear that Informant G feels very strongly about the benefits, or lack thereof, when giving personal data to brands. In contrast, Informant Q admits to seeing some rewards, but relies on a heuristic, or a rule not to disclose personal data to brands. She claims, "[Brands] only need an email, birthdate to send the freebies. [Brands] don't need anything else." Thus, she admits to loving "freebies", but always evaluates how free a "freebie" actually is in terms of privacy cost. Thus, protectionists are characterized by the lack of value concern and a high concern for consumer privacy, as well as the automatic decision to reject personal data disclosure requests.

Capitalists

Informants that fall into the capitalist quadrant exhibit a keen understanding that their personal data are a commodity that they can trade for a range of benefits. For example, Informant E explains how she sees her personal data:

> I drive a Chevy Blazer that costs $75 to fill up, so I might as well get some reward in addition to the utility I already get from purchasing food or whatever or gas. And if I can get more and it's not totally free, because I am trading in my information but it feels free. So it seems like a win-win. I used my points to buy gas and other stuff… So I get free stuff and I like free stuff. (Informant E)

She explains she does not mind providing her personal data to brands, especially when the data collection happens during her regular shopping routine.

Capitalists are not concerned with consumer privacy and actively seek out value. For example, Informant W in responding to how she feels about brands asking for her data, "I feel it's not necessary but they insist and I really need that card because the points there are very helpful." Later Informant W elaborates on the value she receives from a particular loyalty card, when she says, "I will get more opportunities of like when the new [fashion] collection comes, [the brand] will have champagne parties or something and they have sales" and, "I love it [that] for my birthday, they sent me a Happy Birthday card and discounted everything for three days." Thus, for informant W,

the value she gets outweighs any consumer privacy concern she may have. In another interview, Informant K says in response to a clarification question about the reasons for disclosing personal data to brands, “No, absolutely and I don’t mind them having my personal information because I get a lot of benefits from it.” Informant E adds a reason behind this lack of concern for consumer privacy when she says,

> I think actually for the most part firms are collecting information so they can grow their business, so they can target demographics and kind of maximize their earning potential because they are able to find out exactly what you need, when you need it, and how much you want to spend, and then deliver that to you and they can do better themselves. (Informant E)

Thus, she theorizes that brands are collecting this data for both their own benefit (i.e., to increase profitability), but also for consumers’ benefit to serve their needs better.

Many capitalist informants exhibit high degrees of trust in brands, as Informant E goes on to state “I don’t think that anyone really wants personal information so that they can bring you harm”. Similarly, Informant C reveals that he trusts business more than government when he said, “So actually I am far more scared of the police and other [government] services and things like that, than I am of people, who like me, are businessmen just trying to sell something.” Informant B echoes this reasoning by saying, “You know, I would probably say if you are going to over share stick with trusted companies that you know its probably going to be okay.” Informant B further explains that there are implicit contracts between brands and disclosing consumers, when he elaborates,

> I assume based on the kind of implicit honor system here that if I give you information for a purpose, that is what you are going to use it for and kind of for nothing else, unless you ask me. Those to me are kind of implicit rules of engagement and as long as everybody sticks to that, we are cool. (Informant B)

Informant Q goes further and talks about the recourse modern consumers have with social media networks by claiming that,

> I just think you can get a lot of hype generated about a well-known brand, because it is like they made a mistake here, and people always

> going to be on a wagon with that. It is not really my personality to do that, but if it came ultimately to that, you know, if they sold my personal information and someone hacked my bank account or something, then I think I would make a big fuss over it. (Informant Q)

Thus, capitalists not only seem to trust the brands they provide data to, some see it as creating a contract between that brand and them, as well as having recourse methods if that brand does not honor the terms.

Outside of the contract metaphor, other capitalist informants show their high levels of trust in brands. For example, Informant C provides insight into how capitalists interpret customer surveillance by stating,

> That is [marketing's] job. Their motive is to sell things of a certain value and they are using technology that is available to them. I am a technologist as you know but every technology has got its good and evil. Nuclear technology can be used to make nuclear bombs or to make nuclear power plants and it depends on how you use it. (Informant C)

Thus, capitalists are not only characterized by trusting brands with their personal data, but they also lack the emotive responses of the protectionists in response to consumer privacy threats.

Many capitalist informants are well aware of customer surveillance in their lives, but their trust in brands may weaken their concern for consumer privacy. Informant T provides a little more clarity on whether or not she believes that brand requests for her personal data are truly privacy concerns for her. In responding to a question about brands collecting her data at retail stores, she says,

> Sometimes [they ask for] like your birth date so they can send you a little birthday greeting, but I tend not to want to give my information partly because I don't want the spam emails. I just in the end, I think it will drive me to shop more, but yeah, I just. Is it a privacy thing? I don't know if it is so much of a privacy concern. It is more of my concern in terms of 'I don't want your email and I don't want to be part of your club', but I don't know that I am concerned about them knowing that I shop at [their store]. (Informant T)

This line of reasoning is echoed in Informant K's comment when discussing any worries she has over disclosing personal data to brands when she explains,

> It is an irritation. It is not that I think that they are going to you know use information of mine against me, or some kind of conspiracy theory against us or something like that that. It is more just out of irritation that I wouldn't give my details, than out of real concern form my personal safety or privacy. (Informant K)

Thus, for Informants T and K, as well as many other capitalists, disclosure requests are turned down not for consumer privacy reasons, but for the lack of explicit utility expressed as irritation.

Capitalists seek both utilitarian and hedonic value. For example in discussing point cards, Informant O states, "You can get more recognition and you can feel special… some just like the shiny card, they're just fun, like this one for [brand name], you know, it's cool." Thus, he describes hedonic benefits (e.g., feeling special, getting recognition) he experiences from being a target of customer surveillance. Then, he goes on to outline utilitarian benefits by explaining,

> It's ironic that… I don't carry the cards with me, but it is still nice to see them and like checking in on an airliner or boarding first on the airliner, the big one for that, especially domestically, is being able to get access to the overhead bin space, because so many times planes are completely full and there is no overhead bin space, so getting on first you will at least get your bag on the plane which is useful. (Informant O)

These statements detailing the seeking of hedonic and utilitarian value are typical of the capitalist informants.

In fact, many capitalists claim that they wish that customer surveillance activities were even more pervasive, as they often make the consumption experience easier. Informant K states, "I like [Internet] cookies because I love to get targeted at, and so I don't mind for Google or whatever to know what I am searching because it is going to make my online experience better." Informant O agrees with this opinion as he says in frustration,

> If [brands] are smart, I am like, why are you wasting my time, you could be getting this data from other data sources… you know where I live, so why are you asking for this [stuff]? It pisses me off when they are not smart about it. (Informant O)

Informant O goes on to explain,

> It's annoying if you go to a hotel and they don't recognize that you've stayed there before, let alone recognize that you've been to the chain before. It's always nice on an airplane when you get on, 'Welcome back Mr. [Last Name]'. (Informant O)

Thus, if explicit hedonic or utilitarian benefits are evident, capitalists do not consider consumer privacy concerns and automatically choose to disclose personal data.

Pragmatists

Pragmatists are characterized by both high concerns for consumer privacy and value. These informants carefully evaluate each instance of customer surveillance they encounter to assess consumer privacy risks and potential value. For example, Informant D advises,

> Depending on whether or not you like to buy things at those companies, you have the right to choose whether or not you want to give your information and whether or not what they give you back in exchange for your information something you value. So you are selling your information. It is a give and take. That is why I say it is a give and take. See how much your think your information is worth. (Informant D)

For him, personal data are commodities of value that needs to be protected and shared only for worthy benefits. Informant H discusses the tradeoff between consumer privacy and value, when he says,

> I don't mind it if the service is going to be useful to me… when they collect my information and then they give it back to me or they spit it back to me in some way, if it useful to me in a sense I feel I like this brand or I like this product or they are actually using the information in a meaningful way. Then I don't mind… but I don't like to know that they have got all these records out there… because I don't want just because I shop once on a website or into some random shop to buy something, I don't want to be on their database and be there for 5,

> 10, 15 years… I just don't want all this information out there about myself. So I am careful about who I give my information to. (Informant H)

He recognizes that there are valuable benefits, especially with brands he uses frequently, but is also worried about his personal data being kept by brands that he does not have a close relationship to. Informant D and H are typical pragmatists, as they carefully weight the benefits and the risks of providing personal data to brands.

But value is not the only aspect that pragmatists consider when deciding to provide data. Informant X gives us some additional insight, when she explains,

> I would never ever, ever give my details to… any kind of company that in my consideration is unethical… Because it's just, in my head, I don't like them as a company because it's unethical to me what they are doing and therefore I kind of make this association that I don't trust them in terms of my details. (Informant X)

Informant X seems to understand the value of her personal data but she will only disclose to brands that she feels are ethical. Similarly, Informant L talks about being loyal to a brand as being an important consideration in disclosing personal data, when she details,

> I don't want them to know about personal stuff and it's a retail store… If I'm very loyal to the store and I really like them and I'm their loyal customer, then I give my information… [The store] sends me promotional stuff too, right. So I feel like I want to part of their list and they actually mailed [promotional materials] to me. So they have to have my information. (Informant L)

The informant provides her for disclosing personal data, as she enjoys receiving physical mailed promotional offers from a retail store that she is loyal to. Similar to protectionists, pragmatists, such as Informants L and X, consider both brand characteristics and loyalty when making the decision to disclose personal data.

Pragmatists are also characterized by a high degree of value concern. Informant D explains how he negotiates consumer privacy and value concerns:

> I want to know what they want it for and if they don't give me a very good answer, then I won't give out my information to them. Just because they ask, we don't have to give… in a give and take situation, you get something out of it, at the same time, you don't have to. (Informant D)

Thus, awareness of the purpose of the data request and the potential value of being a target of customer surveillance are very important considerations to Informant D. Similarly, Informant H describes his reasons for not using airline point programs,

> Because I am so price driven, so I am not going to stick with [one specific airline]. In the past, I used to fly with certain airlines just for the points, but now it doesn't make sense to because it is so hard to accumulate enough points. So it doesn't make sense. (Informant H)

Pragmatists require clear evidence of potential value in exchange for their data, similar to capitalists. It is the complex relationship between the competing high personal concerns for consumer privacy and value that force pragmatists to cognitively consider each case of customer surveillance.

Apathists

Apathists are theoretically characterized by having a low concern for both consumer privacy and value. Even though there were just two informants that exhibited this archetype, they are important to include as they provide a contrast to the other three archetypes. Because of their lack of consumer privacy concern, apathists do not mind sharing their personal data, including surveillance that tracks their behavior. For example, Informant S repeatedly responded "No" or "No, I think I am fine with that" to questions about retail brands, such as his local grocery store or Amazon, tracking his purchasing and shopping behavior. He explains,

> For example, the [brands] like Safeway and stuff like that doesn't matter what I buy because it could help the company or however they want or why the want to track like whether it is to know people are going to buy this much stuff, etc. and that could help them to know how much to they should buy or produce that much stuff, I don't know. Maybe it is because I may not buy stuff that I am afraid that other people would know you know. I buy other stuff then maybe, but so I don't care. (Informant S)

Informant S is similar to many capitalist informants on his view on consumer privacy in both theorizing the purpose of customer surveillance, and also his notion that he has nothing to hide. Informant V further describes her beliefs, "In fact I think it's not about caring or not about [consumer privacy], because we live in the 21st century, we always need to provide some data, and I don't think it is very serious." Informant V reports that while she feels a lack of control over personal data, she thinks that disclosing personal data are requirements of being part of modern society.

In terms of responding to personal data requests, Informant S sometimes uses an obfuscation strategy, however this is not out of privacy concern, but because of the hassle of providing this data. In one instance he says,

> I don't want stuff sent to me because I guess when you move [companies or home] you are going to have a lot of mail coming and then you have to forward the emails, or forward your mail to your new place. I still get mail at [my old place]. (Informant S)

He uses this strategy of misinformation like a capitalist, not like a protectionist. Moreover, Informant V describes feeling bored by data requests: "I actually feel sometimes that they're boring, when I have to enter [my data] repeatedly to fill out the forms." These informants describe inconvenience or boredom and a general lack of anxiety regarding customer surveillance. Thus, apathists have a relatively low concern for consumer privacy.

Turning now to the concern for value, both apathetic informants could not quickly recall being part of any point or loyalty programs, but after probing further, both were part a program. Informant S receives a free movie as a reward from the local cinema. Similarly, Informant V gets a free coffee after buying nine coffees at a coffee shop she frequents. However, both explained that they did not seek out these programs, as capitalists would have. Moreover, they did not join other loyalty programs because of some privacy fear, as protectionists exhibited. Thus, these apathetic informants are characterized as having a low concern for value as well as low concern for consumer privacy, and seem to not cognitively consider personal data disclosure requests.

General Discussion

Informants' reported similar definitions of privacy and private personal data, as well as similar theories of the motivations of brands to conduct customer surveillance. Informants also reported very different reactions to customer surveillance that can be segmented into the four archetypes of attitudes towards customer surveillance by evaluating their consumer privacy and value concerns (see Table 2.5).

Table 2.5 Comparison of Attitudes toward Customer Surveillance

Attitude Archetype	Attitude Components		
	Thoughts	Feelings	Intended Behaviors
Protectionists	No trust; need for privacy protection	Feels threatened; surveillance = creepy	Automatically avoid customer surveillance
Capitalists	Implicit contract with brands; trust brands	Enjoys utility & feelings of status	Automatically disclose data if benefit explicit
Pragmatists	Carefully consider the merits of each request	Wants to enjoy benefits; worried about privacy	Calculate net benefits that include privacy costs
Apathists	Do not consider value or privacy big concerns	Bored and annoyed; feel a lack of control	Does not seek value but often provides data

Informants share a general conceptualization of consumer privacy, even though they might have slightly different definitions of what personal data are to them. Informants generally have similar theories on brands' motivations to conduct customer surveillance. These results mirror findings in empirical cross-cultural (Newell 1998), cross-generational (Kwasny, Caine, Rogers, & Fisk 2008), and cross-gender research (Kwasny et al. 2008) that definitions of privacy and theories of surveillance motivations are similar across groups, but privacy attitudes vary between these groups.

Despite these variations in informants' attitudes toward customer surveillance, many reported using a variety of obfuscation strategies in the interviews. However, for the most part, these strategies were employed for very different reasons. Protectionist informants, for example, gave false or confusing data to brands in order to protect their personal privacy. Capitalist informants, in contrast, gave misleading data to prevent potential irritation from brands that did not provide explicit value in return for their personal data. This result confirms a similar empirical finding from a survey of Internet

users (Milne & Culnan 2004) that participants are either concerned for their data privacy or avoiding the irritation of junk email communication.

While many informants expressed their consumer privacy concerns, namely protectionists and pragmatists, those classified as capitalist and apatheist did not report being very concerned about consumer privacy. This finding supports many empirical articles (Milne & Bahl 2013; Dinev & Hart 2006; Malhotra et al. 2004; Phelps, Nowak, & Ferrell 2000) that claim that individuals have different responses to privacy and privacy threats.

Similar to privacy calculus research (Xu et al. 2011; Dinev & Hart 2006), high consumer privacy concerns seem to be competing with high value concerns for pragmatist suggesting a deliberate cognitive decision process. However for the other three informant segments, consumer privacy and value concerns were found to be different levels, thus decisions to disclose are likely to be automatic and not calculated. For example, protectionists would not be satisfied with additional value for personal data, as consumer privacy concerns cannot be diminished or subdued by increased value. Similarly, capitalists operate in the exact opposite fashion, where providing more consumer privacy assurance does not motivate increased disclosure of personal data, as they respond to value opportunities. Thus, protectionist and capitalist informants likely make automatic decisions based on consumer privacy and value heuristics respectively. Furthermore, regardless of the potential value offered for personal data or the consumer privacy threats, apatheist informants do not consider these personal concerns when making the decision to disclose data. These findings lend empirical support for the four archetypes of the attitude toward customer surveillance that frame the decision to disclose personal data to brands in either a cognitive or automatic way.

2.4. Managerial Implications

Attitudes toward customer surveillance are important for brands to consider when making decisions on customer surveillance activities, consumer privacy policies consumer segment targeting, or customer surveillance disaster response. Informants in all archetypes advised brands to be more transparent and explicit about consumer

privacy risks and benefits' value derived from disclosing personal data. Many informants admitted that they do not read the privacy statements presented to them by brands online and in person. This advice is not supported by the findings of Hui, Teo, and Lee (2007), as these authors find that the presentation of a lengthy privacy policy to a consumer encourages personal data disclosure more than the presentation of a simply security or privacy seal. Yet, in light of the potential automatic effects of attitudes towards customer surveillance, making the corporate privacy policy data more easily readable by identifying explicit risks and benefits might alert or awaken the rational cognitive decision process instead of a lengthy privacy policy that some consumers do not process rationally and rely instead on often heuristics. The following paragraphs outline managerial implications for each archetype.

Protectionist consumers are chiefly concerned with consumer privacy risks. Therefore highlighting exactly how their personal data would be collected, stored, and used, as well as assurances of data security might allay some of these concerns. Brands might target these consumers by offering specific, customized services to ensure that their personal data are respected. For example, protectionists might pay a premium for a credit card that collects no additional data and deletes or refreshes transaction history frequently.

Capitalist consumers care mostly about deriving the most value out of their data resources. Highlighting the various benefits available by providing their personal data would be very attractive to capitalists. Using a credit card example again, capitalists might prefer an offer that included location-specific personalized services and discounts for disclosing real-time location data to the credit card company.

The competing high consumer privacy and high value concerns might lead pragmatist consumers to yearn for a clear and explicit account of the privacy risks and potential value in the disclosure of data to a brand. While the apathists may not worry about either consumer privacy or potential value, these consumers do likely worry about other brand attributes, such as for example corporate social responsibility, corporate ethics, and brand reputation. If brands are sensitive to consumer segments that exhibit one of these archetypes by enhanced privacy protection services, more explicit value

offerings, or more clear information about the risks and benefits, they may successfully attract and retain those consumers.

2.5. Limitations and Future Research Directions

The major limitation of these studies, and qualitative research in general, is the lack of generalizability. In order to achieve a deep, rich understanding of a specific phenomenon, generalizability is sacrificed (Creswell 2009; Arnold & Price 2006). Efforts were made to have a heterogeneous informant sample in terms of gender, age, occupation, and national culture. This informant sample provided depth into the four archetypes, but individual findings may vary in a large sample. This lack of generalizability presents an interesting direction for future research into attitudes toward customer surveillance. For example, each segment of these attitudes could be examined to define boundary conditions between the segments, to examine how stable are consumers in their attitude segment over time, and to investigate the influence of national culture.

Future customer surveillance research could develop measurement tools to assess these attitudes in specific targeted groups (e.g., deal-prone consumers, highly privacy concerned consumers, seniors, teenagers, Facebook users, Safeway customers). It would be interesting to test of the strength of this attitude's effect on the attitude towards a specific brand in various contexts and situations (e.g., Chinese consumers vs. North American consumers, strong brand attachment vs. weak brand attachment, online consumers vs. offline consumers, wine drinkers vs. beer drinkers). These tools could be used to identify apathists, which were underrepresented in the sample, in order to further explore this archetype. Also, these tools could be used to measure sample populations to provide consumer privacy policy directions for decision makers in corporations and governments.

More research is needed to investigate the tenuous connection between attitudes toward consumer surveillance and attitudes toward general or government surveillance. Further research could explore other influential factors and psychographic variables that

may impact the relationship between consumer surveillance and surveillance in other contexts.

Future research in additional contexts is needed to further study the personal concern for value outside of marketing price promotions. This paper has studied consumers' sense of value in the context of personal data disclosure. Value concern could be examined to determine the different motivational aspects of hedonic and utilitarian benefits. The insights could be applied to consumer gamification, marketing communications, brand positioning, and other marketing strategies.

This paper has provided a boundary to the utility of the privacy calculus concept. From the responses of some informants, the decision to disclose data is likely not a rational cognitive choice that critically weights the pros and cons for some consumers. Rather, this decision to disclose personal data to brands is made automatically depending on the levels of an individual's consumer privacy and value concerns. However, more research into the automatic decisions to or not to disclose data is needed, as well as under what conditions the cognitive decision is cued and supersedes the automatic decision.

Lastly, in the age of big data, different consumer surveillance methods of collecting, storing, and using market intelligence might increase or allay consumer privacy concerns. More research is needed to understand consumer privacy concerns in order to better design corporate privacy policies that are customized to attractive consumer groups.

2.6. Conclusions

This paper provides several contributions to the academic literature and marketing practice. First, the theory section summarizes both the literature on customer surveillance across a broad array of business and social science disciplines. Second, this paper moves the literature beyond the privacy calculus concept, which focuses on rational decision-making, and introduces attitudes towards customer surveillance have both rational and automatic effects on consumer behavior. Third, the personal concerns

of consumer privacy and value were both theoretically and empirically advanced in scope and depth. Fourth, these attitudes were categorized into four archetypes based on consumer privacy and value concerns variations and empirically investigated. And sixth, the paper closes with a research agenda calls for future research into customer surveillance.

Chapter 3.

Smarter Market Intelligence

3.1. Introduction

Many brands collect and capture more customer data from consumers than ever before through *customer surveillance*, or the collection, usage, and storage of customer data (Lyon 2007; Andrejevic 2007; Turow 2008). Customer surveillance is increasingly less obtrusive, less costly, and more data rich due to advances in technology (e.g., facial emotion recognition scanners, location tracking devices, social media platforms; Bauman & Lyon 2013). Collected customer data forms a brand's *market intelligence* resources, or data about the needs, preferences, characteristics, behavior, attitudes, and other attributes of customers (Kohli & Jaworski 1990). Customer insights derived from market intelligence have been shown to improve brand performance (McAffee & Brynjolfsson 2012; LaValle et al. 2011) by allowing brands to, for example, design and test new products, evaluate advertising strategies, and forecast future customer demand for products (Puccinelli et al 2009).

Customer surveillance sometimes evokes customers' privacy concerns, especially when central data are willingly or unwillingly disclosed to a brand without an intimate customer relationship (Marshall 1972). If customers think or feel that their personal privacy has been threatened by a brand, their relationship with that brand can be damaged. To mitigate these customer relationship risks and thus also provide additional value, some brands provide incentives to encourage data disclosure (e.g., immediate discounts, valuable points, access to exclusive information, additional convenience, enhanced service; Andrejevic 2007). Brands are challenged to find the right customer surveillance balance between gaining market intelligence and preserving customer relationships.

Brands need to rethink surveillance activities that collect and capture a wide scope of customer data and develop more efficient market intelligence strategies that still meet brands' data needs, but also protect customer relationships. By eliminating some customer surveillance activities, brands have increased flexibility to select more effective data sources that better meet their data needs. In doing so, brands can increase the effectiveness of market intelligence resources that provide the customer insights that keep their products and services competitive while protecting customer relationships.

This paper theoretically and empirically explores the semantic value of customer data collected from transaction (e.g., credit card statements) and social media (e.g., Facebook) sources to aid market intelligence analytics. It proposes a framework that structures market intelligence resources using seven surveillance prompts (who, what, where, when, why, how, and outcome) that guide the choice of customer surveillance activities and customer data sources to answer these prompts. Using this framework, customer data can be evaluated in terms of how well they predict specific customer insights by exploring data fit factors (data quantity, detail, content, and duality). Then, four experiments explore this model and the contribution of the data fit factors to predict customer insights using transaction and social media data. The paper then discusses the experimental results and concludes with implications for academic research and marketing practice.

3.2. Theory Development

Brands use customer data to design, evaluate, promote, and refine their products and services so they better meet customer needs, but sometimes customers resent having their personal data collected. This section first discusses this customer surveillance paradox from a customer relationship perspective, and then proposes the surveillance prompt framework. The section then develops a model of customer insight value that explores the potential contribution of data fit factors in terms of the accuracy and consistency of customer insight predictions.

3.2.1. Obtaining Customer Data While Protecting Relationships

Marketing strategies based on market intelligence generally outperform strategies based on managerial intuition or experience (LaValle et al. 2011; McAfee & Brynjolfsson 2012). Through an enhanced understanding of customers, market-oriented brands often perform better than product-oriented because of their ability to produce products and services that better meet customers' needs (Jaworski & Kohli 1993; Kohli & Jaworski 1990). By generating, disseminating, and responding to customer insights derived from market intelligence, employee commitment to the brand (Jaworski & Kohli 1993), customer satisfaction (Harter et al. 2002), and customer loyalty (Salanova et al. 2005) have all been shown to increase. These positive outcomes of market intelligence enable brands to build long-term, intimate, and profitable customer relationships.

Built on trust and commitment, customer relationships underpin customer loyalty and customer satisfaction (Morgan & Hunt 1994). Customer trust refers to customers' confidence that a brand is reliable and has integrity (Morgan & Hunt 1994). Customer commitment describes the importance of the relationship to customers and that they devote resources to maintain and perhaps enhance this relationship (Morgan & Hunt 1994). If customers perceive a brand to be reliable and honest, in addition to the feeling that the relationship with the brand is important and valuable, an intimate, long-term customer relationship is likely with that brand.

If customers experience privacy threats from customer surveillance activities, the relationship with the offending brand may suffer. However, customers may not always deem personal data as private in all contexts. Personal data becomes private when data are considered highly central to a customer's identity (e.g., birth date, sexual orientation, relationship status, address, credit card, health records; Marshall 1972). Private data are disclosed to trusted others where an intimate relationship between the discloser and the receiver exists (Marshall 1972). Since customers have intimate relationships with some brands (Fournier 1988), customers may experience privacy threats if that trust is broken by a brand perceived to be not acting with integrity concerning customers' data (Turow 2008). Alternatively, customers may also experience privacy threats when private data are disclosed, often without explicit permission, to other unknown parties (Lyon 2007).

In light of this, brands may offer incentives (e.g., discounts, privileged information, enhanced service, improved convenience) to entice customers to disclose personal data by increasing the immediate perceived value of disclosing data (Culnan & Bies 2003). Brands hope that these incentives may influence the decision to disclose personal data in their favor and also hopefully mitigate the negative impact on customer relationships (Culnan & Bies 2003).

In short, gathering marketing intelligence through customer surveillance is a basic function of market-oriented brands that enables the production of enhanced products and services that better meet customers' needs. Meeting customers' needs allows customer relationships to be established or enhanced that are built on trust and commitment. To prevent privacy threats that may damage or destroy customer relationships, customer surveillance must be thoughtfully conducted and also perhaps infused with additional customer benefits. Brands walk a fine line between the need for market intelligence and the risk of damaging customer relationships.

3.2.2. Rethinking Market Intelligence Strategies

Since market intelligence is linked to brand performance (Jaworski & Kohli 1993), customer surveillance has become a central aspect of marketing operations and investments (e.g., customer relationship management (CRM) systems). But many brands are conducting customer surveillance activities without clear strategies that meets the brand's data needs at the same time as being sensitive to customers' privacy concerns (Turow 2008). This lack of a market intelligence strategy may threaten customer relationships and is exacerbated by technological advances that have made customer surveillance more powerful and less visible (Bauman & Lyon 2013). The following paragraphs present the surveillance prompt framework that aids in the strategic design of market intelligence resources so that customer insights can be generated with less customer surveillance.

Surveillance prompts store discrete customer facts collected by customer surveillance activities using a set of generic questions or prompts (i.e. when, where, what, how, who, why, outcome; Thomsen, 1997; Bisdikian et al. 2009). "*When*" uncovers

the temporal nature of customer behavior by understanding the frequency, time, or date of customer activity. "*Where*" holds the physical or virtual locations of customers. "*What*" is essential for brands to manage inventory stocks and also to determine which offerings are frequently bought (or not bought) together. "*How*" aids the understanding of customers' preferred methods of customer activity, including shopping orientations, payment type choices, and other potential customer (dis)satisfaction points. "*Who*" can be used to create unique customer profiles that might include characteristics such as interests, demographics, psychographics, memberships, and links to other customers. Together these surveillance prompts provide a picture of customer behavior from a variety of different perspectives that can yield many valuable customer insights.

These surveillance prompts are independent of customer surveillance technologies, as data could be gathered using a variety or a combination of technologies to answer a prompt (see Table 3.1). By focusing on the answers to the prompts and customer insights and not the specific source or the surveillance technology employed, this framework is appropriate in the current and also future technological environments.

Table 3.1 Surveillance Prompts Framework

Surveillance Prompt	Customer Data Example	Possible Customer Data Source
When?	June 3, 2015 at 9:12am	Transaction
Where?	Waterloo Station, London, UK	Transaction or Social Media check in
What?	2 black coffees & 2 croissants	Transaction
How?	Debit card number	Transaction
Who?	Loyalty number or Facebook update	Transaction or Social Media check in
Why?	Meeting a friend for breakfast	Social Media check in
Outcome?	Revenue of £5.50 (approx. C$10.35)	Transaction

Many of these surveillance prompts can be answered with routine point of purchase transaction data, as is illustrated by Table 3.1. To add further depth and to aid understanding, these transaction data could be augmented with sensors data (e.g., face recognition, RFID tags) to extract additional and perhaps more precise data. But even with additional sensor data, transaction data provides limited understanding of customers' motivations (i.e., why). Customers' motivations are difficult to obtain without directly surveying customers. But self-reported survey methods may have measurement

issues that bias findings (e.g., social desirability bias, expectation bias; Creswell 2009). Social media offer a potential solution, as they may provide clues to customers' motivations in customer forums, check in to locations, and profile histories (Kietzmann et al 2011). These data can be mined to identify possible motivators and married with other data to potentially give a more complete and detailed picture of customers (Bauman & Lyon 2013).

Marketers cannot possibly anticipate all the potential questions that they may need to ask of the data in the future. By designing marketing intelligence resources using surveillance prompts and strategically selecting appropriate customer data sources that answer these prompts, brands will have the data needed to develop valuable customer insights (Watson, 2013). In doing so, brands can examine their customer surveillance activities and reduce those activities that do not add value to their market intelligence resources.

3.2.3. Customer Insight Value

Since there is a potential risk to customer relationships, brands must be strategic in the design of market intelligence by seeking customer data that accurately and consistently predict customer insights. *Customer insights* are identified patterns in customer data that indicate customers' personalities, future purchases, preferences, needs, and other customer attributes (Kohli and Jaworski 1990). The following paragraphs explore how customer data attributes or data fit factors (data quantity, detail, content, and duality) add value to customer insights in terms of prediction accuracy and consistency.

Social scientists have been long concerned with showing that their conclusions and predictions are precise or correct. The constructivist approach to accuracy has been widely used in past research (Hall, Ariss, & Todorov 2007; Funder 1995), and it examines the level of agreement or consistency among individual judges (Kruglanski 1989; Funder 1995). Prediction consistency refers to the degree to which individual predictions of customer attributes agree with one another. Since many judges can agree on a prediction and yet still be incorrect, prediction accuracy is also key to customer

insight value. Prediction accuracy can be measured using trusted comparison values from other sources of data that are deemed to be (more) accurate. Thus, prediction accuracy and consistency are two important factors that can be used to measure a predicted customer insight's value.

Brands are keenly interested in predicting a range of customer insights, including personality characteristics (i.e., who) and future purchases (i.e., what), to improve the effectiveness and efficiency of marketing strategies (Hoch 1988). These predictions are based on judges' attributions, or links between observations and casual explanations, made from examining the customer data available to judges (Folkes 1988). *Data fit* refers to the appropriateness of customer data to predict a customer insight accurately and consistently. This paper explores four data fit factors including data quantity, detail, content, and duality.

Data quantity and detail are important data attributes to assess the knowledge contained in a set of data. If judges have more knowledge about the subject of the data, empirical evidence shows that those judges make more accurate and consistent predictions of customer insights than judges with less knowledge (Funder 1995; Funder & Colvin 1988). *Data quantity* refers to the shear amount of data points in a dataset. *Data detail* involves the specificity of the data points in a dataset. Customer data sources that are high in both quantity and detail contain more potential knowledge about customers, and thus may provide more accurate and consistent predictions of some customer insights.

Data content describes the subject matter or substance of a dataset. Although there are other forms of customer data (see Plangger & Watson 2015), this paper specifically examines social media and transaction data in the context of predicting personality characteristics or future purchase behavior. Individuals predict personality characteristics very quickly after first meeting a new person even without preexisting knowledge about that person. These predictions are often fairly consistent and accurate impressions of that person's personality (Uleman 1999; Kahneman & Tversky 1973). But future behavior predictions require more knowledge about the past behavior of that

person, as measures of past behavior have been shown to improve to future behavior predictions (Ajzen 2011).

Data duality refers to the merging of social media data and transaction data. Dual source data may positively impact accuracy and consistency of some predicted customer insights due to the complementary dual source data that may overcome knowledge gaps with single source data. Past purchase transaction data may seem objective since it records purchase details, but these are only snapshots of customers' past purchase behavior, as captured transaction data does not include, for example, items that the customer either could not find, or found better deals elsewhere (Boyd & Crawford 2012). Furthermore, interpretation problems may exist with social media data, as often behavior is not overt, and also network metrics (e.g., tie numbers, tie strength) are poor markers of true relationships (Boyd & Crawford 2012). While some researchers (Bollier & Firestone 2010; Boyd & Crawford 2012) have classed these drawbacks as poor indicators of true behavior and warn against combining sets of these data, each set of data potentially contains different knowledge and when combined may offer a clearer picture of an individual customer.

While the data content may provide different customer insight values due to the different information contained in the data, the contribution of data quantity and detail to customer insight value should not be overlooked. Due to the self-presented content, social media data may provide more valuable personality predictions than transaction data (Bauman & Lyon 2013). But high quantity and highly detailed transaction data may provide more valuable predictions than relatively low detail social media data with few data points. Similarly, transaction data capture past behavior and thus may provide more valuable purchase behavior predictions than social media data (Azjen 2011), but highly detailed social media data often captures elements of past purchase behavior as well. Data detail, quantity, content, and duality need to be explored together to evaluate which factors significantly contribute to accurate and consistent predictions of customer insights. Thus, I propose:

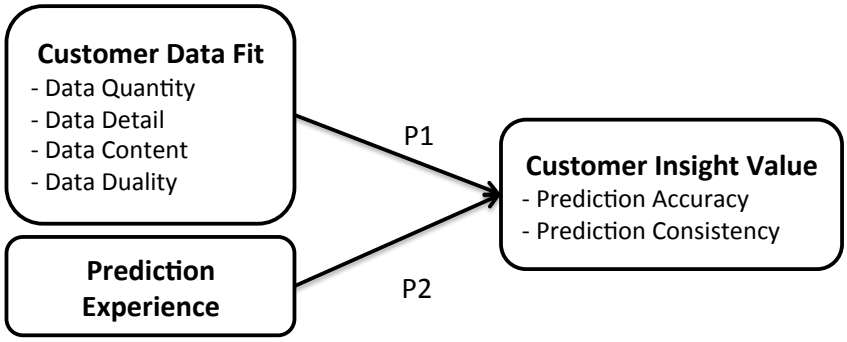
Proposition 1: Customer insight value depends on how well customer data fits the task of predicting a specific customer insight.

As judges repeat the process of predicting customer insights, their predictions are likely to be more accurate and consistent due to *prediction experience*. Prediction experience results in perceptual learning, or "performance improvement in perceptual tasks as a result of practice or training" (Petrov et al. 2005: 715). Perceptual learning produces self-generated feedback that has been shown to be increase accuracy almost as effectively as external feedback (Petrov & Anderson 2005; Petrov et al 2005). Thus, predictions should become more valuable as judges become more experienced predicting customer insights from a customer data source. When comparing judges with little prediction experience and those with some prediction experience, additional prediction experience should have a positive impact on prediction accuracy and consistency that adds to overall customer insight value. Thus, I propose:

Proposition 2: Prediction experience positively impacts predicted customer insight value.

To increase the effectiveness of customer surveillance activities, customer data sources can be evaluated in terms of their value in accurately and consistently predicting customer insights. Data fit factors, including data quantity, detail, content, and duality, together with prediction experience, theoretically contribute to a predicted customer insight's value (see Figure 3.1). This customer insight value model can be described as mid-level theory as it is moderately abstract, but also limited in scope to the practice of predicting customer insights (Kuechler & Vaishnavi 2012; Gregor 2006). The next section details an experimental method that examines this model by exploring the customer data fit factors for two specific customer insights.

Figure 3.1 A Model of Customer Insight Value



3.3. Methods and Results

This section explores customer insight value using four experimental studies identified as 1, 2a, 2b, and 3. By manipulating participants groups, researchers can infer that variations in the measured effects are caused by these manipulations (Creswell 2009). This paper uses experiments that manipulate the customer data that respondents are exposed to in order to identify the contributions of data fit factors and prediction experience to customer insight value (see Table 3.2). Before reporting results, the research method is detailed by outlining the experimental procedures, data conditions, and analysis methods utilized.

Table 3.2 Exploring Customer Insight Value

Customer Insight	Variable Explored	Study Number
Personality	Data quantity	1, 3
	Data detail	
	Data content	
	Data duality	
	Experience	3
Future Purchase Behavior	Data quantity	2a, 2b, 3
	Data detail	
	Data content	
	Data duality	
	Experience	3

Experimental Procedures

In this paper human respondents are used in place of more advanced computers, as algorithms to process these data to predict customer insights have not been invented at the time of writing. Using respondents in this way is a return to manual analysis and interpretation that underpins turning data into knowledge (Fayyad et al. 1996). Respondents are instructed to evaluate an individual's data to make specific predictions about that individual, therefore any English-speaking adult could be a potential respondent. As such, all study participants were recruited from a general Internet consumer panel pool using Amazon.com's Mechanical Turk (mTurk) service with the only restrictions being that they lived in North America and were over 19 years

of age. mTurk is an online marketplace where individuals or "workers" seek simple jobs or tasks for small cash incentives. While not perfectly representative of the North American population, evidence shows that mTurk samples are not dramatically skewed or biased in comparison with other online and offline survey collection methods (Buhrmester et al., 2011; Goodman et al., 2013).

Respondents underwent several tests to both check experimental manipulations and respondents' attention to ensure response quality. They were asked to identify the kind of data they had observed (e.g., Facebook, credit card statements, iTunes records, or other). Also, respondents were asked to select "agree" in a 5-scale point question scaled from "strongly disagree" to "strongly agree" to check attention near the end of the survey. Respondents that failed these checks were deleted from the study's sample. I attempted to recruit 40 respondents for each of the data and customer insight conditions to ensure sufficient statistical power after the removal of incomplete responses and failed manipulation and attention checks.

Respondents were asked to answer an Internet survey that was laid out using the following procedure: (1) accept the informed consent form; (2) observe one of eight sets of an individual's personal data; (3) answer questions to predict a customer insight based on their observations; (4) answer demographics questions. Respondents received a nominal incentive (US$0.60 on average) for their participation to motivate an adequate number of responses.

Respondents in Studies 1 and 3 were asked to observe an individual's personal data and assess that individual's personality using the Gilbert and Warren (1995) personality segmentation scale that includes five dimensions: economizer, credit user, self-confidence, home oriented, and fashionable. This scale was chosen because of its simplicity and the range of identified characteristic dimensions. Moreover, this type of scale choice offers more actionable managerial implications for consumer segmentation than a more general psychology scale (e.g., a Big Five scale).

Studies 2a, 2b, and 3 asked respondents to observe an individual's personal data to assess the likelihood of buying certain brands. The brands in the purchase behavior prediction studies need to be dissimilar enough to allow for potential variation.

To select high and low involvement brands, a pre-test survey was developed that asked 116 respondents to rate brands on perceived value attributes (value for money, functional performance, good service, social status, value expression, and reputation; Sweeney & Soutar 2001). Also, pre-test respondents were asked to assess the likelihood that a consumer would buy brands in combination with one another. From the results, three low purchase involvement brands (Starbucks coffee, Red Bull energy drink, and Miller Lite beer) were selected and used in Study 2a and three high purchase involvement brands (United Airlines business class service, Mercedes vehicles, and Apple iPhone) were selected and used in Studies 2b and 3. Respondents in the studies reported below were asked to assess the purchase likelihood of these brands. To ensure that no one data condition was biased against or for a specific brand, attitudes towards these brands were evaluated prior to observing the data using Homer's (1995) scale. Respondents were randomly placed into a data or task conditions automatically by the survey software.

Data Conditions

Studies used the same eight data conditions that were constructed from four sets of an individual's personal data: one month of credit card statements, three months of iTunes purchase records, public Facebook data using minimal privacy settings, and detailed Facebook data downloaded from Facebook account settings. Participants observed these data either separately (single source) or in combination with each other (dual source) providing eight data conditions that varied in all other data fit factors (see Table 3.3).

Relative customer insight value can be measured by comparing the average prediction accuracy and consistency between data conditions. Using these measures, these studies explore the contribution of data fit factors and prediction experience to customer insight value. The specific customer insights or scores are of little value in the context of this paper, but would be of great value to a brand or in other research contexts. To assess prediction accuracy, comparison scores were collected from the individual who provided the data (self-reported), as well as eight close friends and family. Comparisons of predicted scores and friends and family scores evaluate the accuracy of

personality predictions, as close acquaintances have been shown to have more valid personality predictions than self-reported predictions (Kolar et al. 1996). As they did not observe any of the data provided to experimental respondents, friends and family assessed personality from experiences and interactions with the individual who provided the data for this research. In contrast, purchase behavior predictions were evaluated using self-reported scores, because of the additional personal knowledge about purchase intentions and brand preferences that the individual has access to make his prediction.

Table 3.3 Data Conditions & Customer Data Fit Variables

Data Condition	Data Quantity	Data Detail	Data Content
Credit card	High	Low	Transaction
iTunes	Low	High	Transaction
Facebook public	Low	Low	Social media
Facebook detail	High	High	Social media
Merged low detail	Mixed	Low	Dual source
Merged high quantity	High	Mixed	Dual source
Merged transaction	Mixed	Mixed	Transaction
Merged high detail	Mixed	High	Dual source

Analysis Methods

Data conditions' average prediction accuracy and consistency scores are compared to assess each data condition's relative customer insight value. To assess prediction accuracy, average prediction values from each data condition are compared to the corresponding self-reported or friends and family score. The absolute value of the differences between the predicted and comparison scores of each scale item are summed to provide a measure of how inaccurate the predictions are from the comparison values. Then, analysis of variance (ANOVA) tests on the inaccuracy measure indicate the level of variation between conditions. Planned inaccuracy mean contrasts test the significance of potential data fit factors' (high vs. low data detail/quantity, transaction vs. social media data content, dual vs. single source data) contribution to prediction accuracy. Effect sizes are calculated for all significant data fit factors using Cohen's *d* statistic that corrects for different sample sizes.

To measure prediction consistency, Intra-class Correlation Coefficients (ICCs) are calculated within data conditions that assess prediction reliability by analyzing the variance of predictions within a condition (Bartko 1966; Shrout & Fleiss 1979). ICC is a special case of the popular inter-rater correlation (i.e. weighted kappa: Spitzer et al. 1967; Cohen 1968) that is used to test the reliability of the evaluations of more than one rater or, in this case, respondents. The consistency results reported below use ICC(2), as it eliminates the variance between the respondents and concentrates on the predictions themselves (i.e. the mean respondent error is set to zero) since conditions contain samples of potential respondents. The resulting statistic ranges from zero (i.e. no respondent agreement) to one (i.e. full respondent agreement) and describes the variance that is "real" between the individual predictions. For example, an ICC(2) of 0.60 is interpreted to mean that the respondents agree 60% of the time. A simple average is taken of the ICC(2) statistics within a data condition for comparison with other data conditions.

After prediction accuracy and consistency statistics have been calculated for each data condition, these statistics can be compared in unison with each other to make judgments on the relative customer insight value derived from the data sources. The following four experiments outline the experimental design used and the respondent sample before reporting prediction accuracy, prediction consistency, and customer insight value results.

3.3.1. Study 1: Personality Predictions From Customer Data

Respondents in Study 1 were asked to produce personality predictions using the Gilbert and Warren (1995) scale after observing an individual's personal data. Respondents' personality predictions were evaluated for accuracy using two sets of comparison scores (self-reported and friends and family scores) and assessed for consistency by calculating ICC(2) scores (see Table 2.4). The actual personality prediction scores are not relevant for this study, as the purpose is to compare the accuracy and consistency of scores between data conditions. Initially, 370 survey responses were collected using the mTurk panel service. After cleaning the dataset of incomplete responses, non-unique IP address, and failed manipulation or attention

checks, the resulting cleaned dataset contains 282 responses. This resulted in a useable response rate of 76.2% over all of the data conditions, and no systematic bias was apparent in deleted responses. The sample was 57.9% female, 62.0% under 40 years of age, 50.9% single, and 75.3% of European descent.

Prediction accuracy varied significantly among data conditions in one-way ANOVA tests with both the self-reported ($F_{(7,231)}$=3.960, p<0.001) and Family and Friends ($F_{(7,231)}$=4.031, p<0.001) comparison values (see Table 3.4). Personality predictions are arithmetically closer to friends and family comparison scores than self-reported values. When a runs test is applied, the probability of all eight friends and family inaccuracy comparison values being less than the self-reported is 0.5^8 or 0.0039, which is significant. This finding is in line with the literature (see Kolar et al. 1996) and indicates the difficulty of individuals have to objectively assess their own personality.

Table 3.4 Study 1 Prediction Results

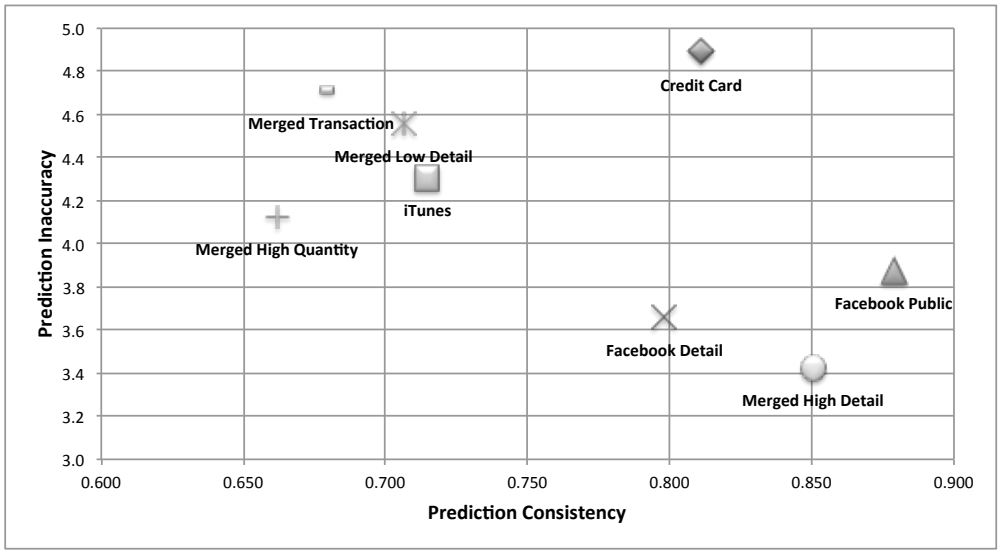
Data Condition	Responses	Inaccuracy		Consistency
		Self	F&F	
Credit card	38	6.23	4.89	0.811
iTunes	33	5.61	4.31	0.715
Facebook public	37	5.60	3.88	0.879
Facebook detail	40	5.01	3.66	0.798
Merged Low detail	39	5.97	4.56	0.706
Merged High quantity	27	5.26	4.13	0.662
Merged transaction	30	6.05	4.71	0.677
Merged high detail	38	4.61	3.43	0.850
Study total	282			

Planned inaccuracy mean contrasts reveal that social media data content had a significant impact on prediction inaccuracy (social media vs. transaction: $t_{(231)}$=-3.335, p=0.001, d_{Cohen}=0.588), but data quantity (high vs. low: $t_{(231)}$=0.731, p=0.465), data detail (high vs. low: $t_{(231)}$=1.605, p=0.110), and data duality (dual vs. single source: $t_{(231)}$=1.331, p=0.184) did not. Data content appeared to be the only factor that had any impact on personality prediction consistency, as predictions made with social media data (ICC(2) = 0.839) are arithmetically more consistent on average that those made with transaction

data (ICC(2) = 0.763)[1]. Other data fit factors did not appear to have an impact on prediction consistency.

Study 1 explored both personality prediction accuracy and consistency across eight data conditions and found that social media data provides more accurate and consistent personality predictions than transaction data. By comparing the data conditions in terms of personality prediction accuracy and consistency (see Figure 3.2), two data condition groups and one outlier data condition emerge. One group (merged transaction, merged low detail, iTunes, and merged high quantity) provided relatively inaccurate predictions with a relatively low level of consistency. The other group (Facebook detail, Facebook public, and merged high detail) provided relatively accurate personality predictions with a relatively high degree of consistency. An outlier condition (credit card data) provided relatively inaccurate but consistent personality predictions.

Figure 3.2 Customer Insight Value for Personality Traits



[1] The interesting arithmetic differences are reported here and in subsequent studies, but these differences have not been statistically tested as I am not aware of a statistical test for ICC values.

3.3.2. Study 2a: Low Purchase Involvement Predictions

Study 2a investigates the data fit factors' (data quantity, detail, content, and duality) contribution to accurately and consistently predicting low involvement purchase likelihoods of Starbucks coffee, Red Bull energy drink, and Miller Lite beer. The study assessed accuracy by comparing self-reported scores and predicted scores, as well as consistency by calculating an average ICC(2) within data conditions (see Table 3.5). Initially, 314 responses were collected before removing incomplete responses, failed manipulation checks, failed attention checks, and non-unique responses. These removed responses seemed to be random, as they had no apparent data condition, date, or other systematic bias. This resulted in a cleaned dataset containing 253 unique responses and a useable response rate of 80.6%. Respondents were predominantly male (56.0%), under 40 years of age (73.5%), university educated (79.3%), and half were married (50.0%).

Table 3.5 Study 2a Prediction Results

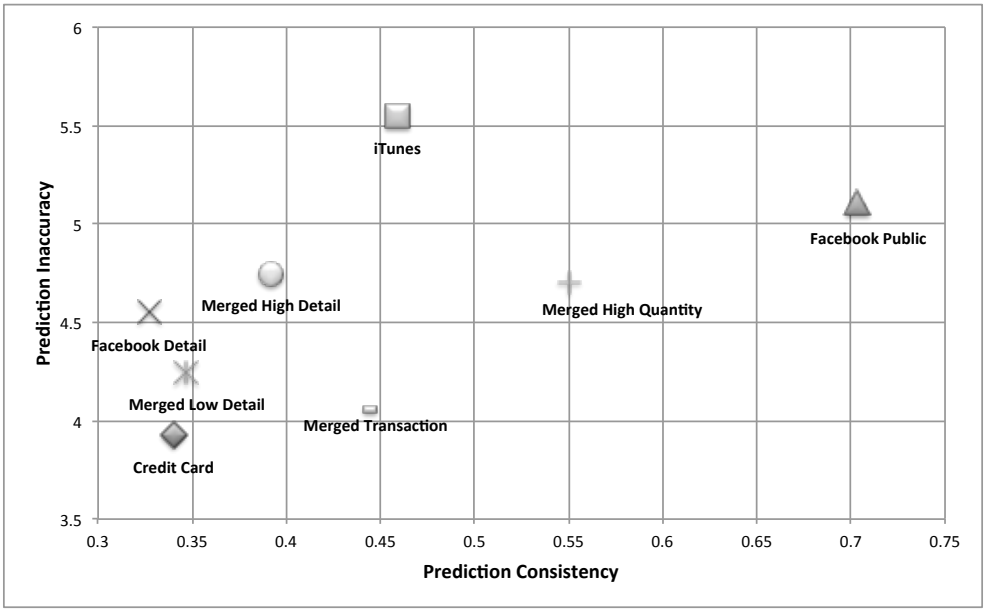
Data Condition	Responses	Inaccuracy	Consistency
Credit card	30	3.93	0.340
iTunes	33	5.55	0.459
Facebook public	36	5.11	0.703
Facebook detail	29	4.55	0.327
Merged low detail	34	4.24	0.347
Merged high quantity	28	4.75	0.392
Merged transaction	33	4.06	0.442
Merged high detail	30	4.70	0.550
Study total	253		

The mean inaccuracy of purchase predictions (see Table 3.5) varied significantly across data conditions, as tested by one-way ANOVA ($F_{(7,9.607)}$=4.630, p<0.001). Planned inaccuracy mean contrasts reveal that both quantity (high vs. low: $t_{(245)}$= -4.249, p<0.001, d_{Cohen}=0.726) and detail (high vs. low: $t_{(245)}$=2.060, p=0.040, d_{Cohen}=0.322) are significant data fit factors when predicting low purchase involvement behavior. Data content (social media vs. transaction: $t_{(245)}$=1.370, p=0.172) and data duality (singe vs. dual source: $t_{(245)}$=0.417, p=0.417) are not significant factors.

Respondents within data conditions produced fairly inconsistent predictions, with Facebook detail and credit card data conditions having the lowest arithmetic consistency scores (see Table 3.5). Both of these data are high quantity conditions, thus data quantity is likely not a contributing factor to prediction consistency in this case. The remaining data fit factors appeared to not contribute to prediction consistency.

Respondents produced significantly more accurate predictions of low purchase involvement behavior by observing low detail and high quantity data sources (e.g. credit card statements), although these predictions are generally less consistent than predictions made from other low quantity sources (see Figure 3.3).

Figure 3.3 Customer Insight Value for Low Involvement Purchases



3.3.3. Study 2b: High Involvement Purchase Predictions

Study 2b asks respondents to predict future purchases of three relatively high purchase involvement brands: United Airlines business class service, Mercedes automobile, and Apple iPhone. Initially, 330 responses were collected before the data was cleaned to remove incomplete responses, failed manipulation checks, and non-unique responses. These removed responses seemed to be random, as they had no apparent data condition, date, or other systematic bias. This resulted in a dataset

containing 277 unique responses and a useable response rate of 83.9%. The sample respondents were predominantly female (60.7%), under 40 years of age (62.2%), university educated (62.3%), of European descent (73.4%), and 42.3% were married.

Table 3.6 Study 2b Prediction Results

Data Condition	Responses	Inaccuracy	Consistency
Credit card	34	4.03	0.759
iTunes	38	5.45	0.461
Facebook public	38	3.68	0.391
Facebook detail	37	5.05	0.407
Merged low detail	34	3.48	0.339
Merged high quantity	32	4.19	0.594
Merged transaction	33	2.97	0.445
Merged high detail	31	3.84	0.339
Study total	277		

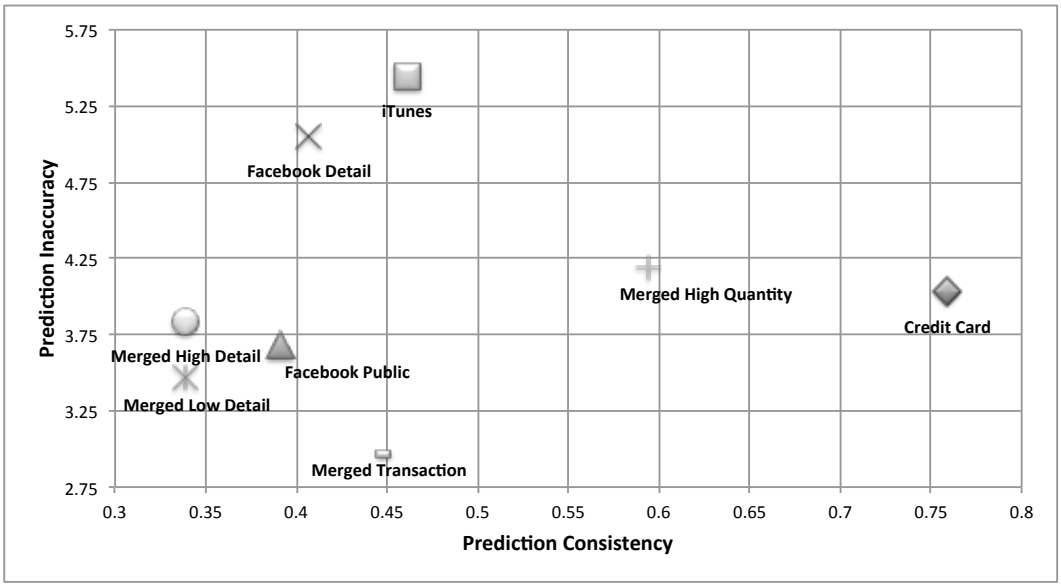
Respondents' predictions varied significantly in terms of average inaccuracy means between data conditions (see Table 3.6) tested by one-way ANOVA ($F_{(7,23.904)}$=4.590, p<0.001). Planned inaccuracy mean contrasts reveal that data detail (high vs. low: $t_{(269)}$=3.699, p<0.001, d_{Cohen}=0.598) is a significant factor in data fit, and data quantity (high vs. low: $t_{(269)}$= -0.064, p=0.949), content (social media vs. transaction: $t_{(269)}$= -0.980, p=0.328), and duality (dual vs. single source: $t_{(269)}$=0.638, p=0.161) are not.

Prediction consistency within data conditions ranged from 0.339 to 0.759 (see Table 3.6). Most data conditions had relatively arithmetically similar average consistency values, except for two outlier data conditions (merged high quantity and credit card) that had comparatively high arithmetic consistency values. Thus, no single data fit factor seems to contribute to prediction consistency for high involvement purchases.

In short, low detail data significantly aid accurate future behavior predictions of high purchase involvement brands, and with the exception of credit card data, behavior predictions were largely inconsistent. In terms of prediction accuracy, a group of data conditions (merged transaction, merged high detail, merged low detail, and Facebook public) performed on par with credit card data (i.e., not statically significant, p>0.050),

although predictions made with credit card data were more arithmetically consistent (see Figure 3.4).

Figure 3.4 Customer Insight Value for High Involvement Purchases



3.3.4. Study 3: Impact Of Prediction Experience

Study 3 investigates the impact of prediction experience on customer insight value (Proposition 2) in an 8 (data conditions) X 2 (prediction experience) experimental design. By altering the sequence of personality (Study 1) and high purchase involvement behavior (Study 2b) prediction tasks, two sets of predictions values were produced that are either made with or without prior prediction experience. Initially, 730 respondents answered the experimental survey, but after cleaning the data for incomplete responses, failed manipulation checks, failed attention checks, and non-unique IP address checks, the study had 621 respondents. This resulted in an 85.1% useable response rate and there appeared to be no apparent bias in removed responses. Study 3 respondents were 51.4% male, 68.3% under 40 years of age, 68.1% university educated, 76.6% of European descent, and 50.7% single.

Two-way ANOVA tests were preformed for both the personality and behavior prediction accuracy to measure the main and interaction effects of the data and prediction experience conditions (see Table 3.7). For personality prediction accuracy,

there was a significant main effect for data conditions ($F_{(7,599)}$=8.577, p<0.001), but both the main effect for prediction experience ($F_{(1,599)}$=3.700, p=0.055) and the interaction effect ($F_{(7,599)}$=1.024, p=0.413) were not significant. For high purchase behavior prediction accuracy, there was a significant main effect of data conditions ($F_{(7,605)}$=4.071, p<0.001), but both the main effect of prediction experience ($F_{(1,605)}$=2.997, p=0.084) and the interaction effect ($F_{(7,605)}$=1.045, p=0.398) were not significant. Thus in both prediction tasks, the data observed had a significant effect on the prediction accuracy, but prediction experience did not have a significant main effect nor was there a significant interaction effect.

Table 3.7 Study 3 Prediction Results

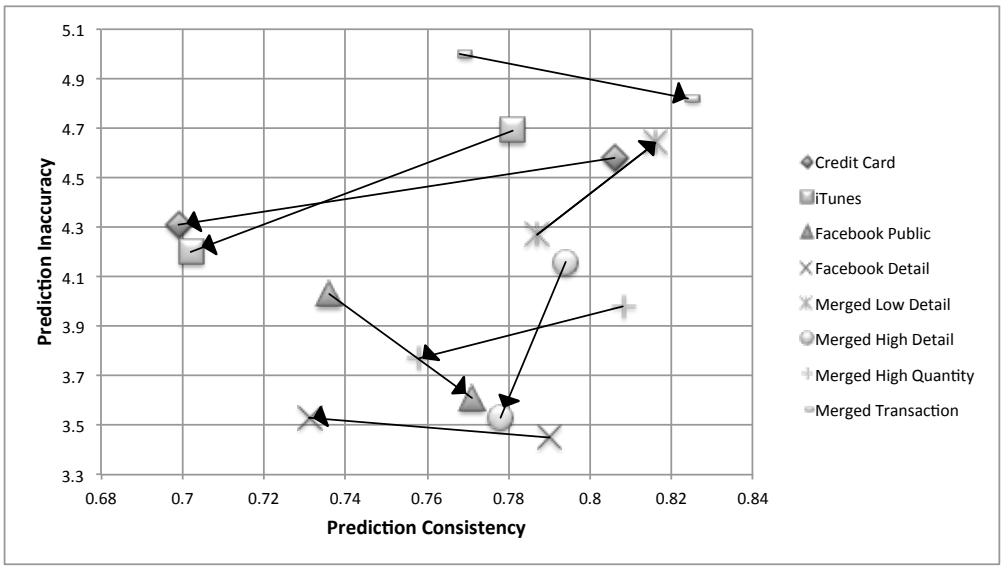
Data Condition	Responses		Personality Predictions				Behavior Predictions			
			Inaccuracy[1]		Consistency[2]		Inaccuracy		Consistency	
	P→B	B→P	P→B	B→P	P→B	B→P	P→B	B→P	P→B	B→P
Credit card	42	37	4.58	4.31	0.806	0.699	2.55	2.97	0.442	0.658
iTunes	49	35	4.69	4.20	0.781	0.702	3.35	3.71	0.513	0.543
Facebook public	44	37	4.03	3.61	0.736	0.771	2.61	3.30	0.593	0.639
Facebook detail	37	40	3.45	3.53	0.790	0.731	2.97	2.80	0.463	0.369
Merged low detail	40	38	4.27	4.64	0.787	0.816	2.75	2.55	0.535	0.632
Merged high quantity	38	36	3.98	3.77	0.808	0.758	2.71	2.63	0.293	0.446
Merged transaction	30	43	5.00	4.82	0.768	0.824	2.23	2.67	0.657	0.534
Merged high detail	40	35	4.16	3.53	0.794	0.778	2.93	3.02	0.468	0.605
Task order	320	301								
Study total	621									

[1]Personality predictions inaccuracy statistics report the difference between the condition mean and corresponding Friends & Family mean value.
[2]Personality prediction consistency statistics are the average ICC(2) statistics for the subscales of the Gilbert and Warren (1995) personality scale.

To provide further evidence of the data fit factors' contributions displayed in the results of Study 1 and 2b, planned inaccuracy mean contrasts were performed separately on personality and high purchase involvement prediction scores. As in Study 1, planned personality prediction inaccuracy mean contrasts reveal that data content is a significant data fit factor (social media vs. transaction: $t_{(607)}$= -6.549, p<0.001, d_{Cohen}= 0.637), but data quantity (high vs. low: $t_{(607)}$= -1.214, p=0.225), detail (high vs. low: $t_{(607)}$= -1.045, p=0.296), and duality (dual vs. single source: $t_{(607)}$= 1.429, p=0.153) are not. Planned purchase behavior prediction inaccuracy mean contrasts reveal that data quantity (high vs. low: $t_{(613)}$= -2.518, p=0.0.12, d_{Cohen}= -0.247) and detail (high vs. low: $t_{(613)}$= 2.247, p=0.025, d_{Cohen}= 0.252) are significant data fit factors, but data content (social media vs. transaction: $t_{(613)}$= -1.385, p=0.167) and duality (dual vs. single source: $t_{(613)}$= 1.205, p=0.229) are not. These findings show the impact of data detail, mirroring Study 2b's findings, but also adds data quantity as a significant data fit factor that adds to prediction accuracy in the context of high involvement purchases.

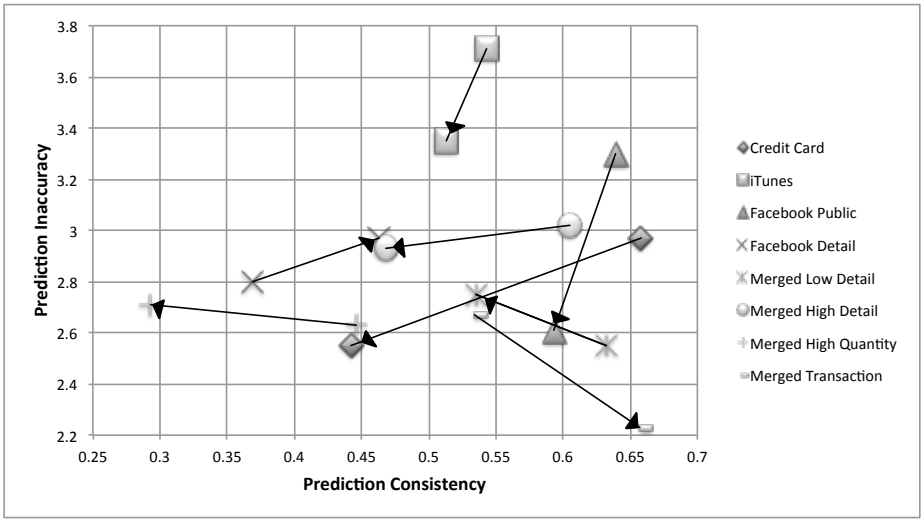
Consistency varied arithmetically more when respondents predicted behavior (0.293 < ICC(2) < 0.658) and less so when predicting personality (0.699 < ICC(2) < 0.824), as is illustrated in Figures 3.5 and 3.6. Prediction experience led to more arithmetically inconsistent personality predictions in 5 out of the 8 data conditions, and 6 of the 8 data conditions when predicting purchase behavior. There are no apparent patterns in both sets of consistency values that point to a specific data fit factor.

Figure 3.5 Data Value for Personality Prediction*



* To distinguish between two prediction experience values, an arrow is drawn from no (P→B) and some (B→P) prediction experience values.

Figure 3.6 Data Value for High Purchase Involvement Prediction*



* To distinguish between two prediction experience values, an arrow is drawn from no (B→P) and some (P→B) prediction experience values.

These results indicate perceptual learning from experience was minimal, thus prediction experience does not significantly contribute to either prediction accuracy or

consistency in both personality and high purchase involvement behavior prediction tasks. For the most part, this study's data fit factor results support the conclusions drawn in previous studies above. The next section discusses, compares, and contrasts the results of all four studies.

3.4. General Discussion

This section compares and contrasts the results of the four experiments to reflect on the contribution of the data fit factors and prediction experience. The following paragraphs separately assess the four data fit factors for their contribution to customer insight value using Cohen's *d* (see Table 3.8). Cohen (1992) offers simple scale to describe the size of effects (small effect *d*=0.2, moderate effect *d*=0.5, and large effect *d*=0.80). The section concludes with an evaluation of the customer insight value model.

Table 3.8 Effect Sizes of Prediction Inaccuracy Determinants[1, 2]

Customer Insight	Significant Data Fit Factors				Prediction Experience[3]
	High Quantity	High Detail	Social Media Content	Dual Source	
Personality	Not significant	Not significant	-0.588 (1) -0.637 (3)	Not significant	- 0.132 (3)
Low Purchase Involvement Behavior	-0.726 (2a)	0.322 (2a)	Not significant	Not significant	Not tested
High Purchase Involvement Behavior	-0.247 (3)	0.598 (2b) 0.252 (3)	Not significant	Not significant	-0.109 (3)

[1]Effect sizes reported are from the study in the parenthesis, i.e. (Study).
[2]Effect sizes reported are calculated using Cohen's *d* that accounts for different sample sizes.
[3]The impact of prediction experience was non-significant in two-way ANOVA tests as reported in Study 3 for both prediction tasks (personality task, *p*=0.055, power analysis = 0.488 with alpha at 0.05; purchase behavior task, *p*=0.084, power analysis = 0.405 with alpha at 0.05).

High quantity data significantly increased future purchase behavior predictions, although not in Study 2b. Data quantity had a moderate effect in Study 2a's (0.726 of a

standard deviation) low purchase involvement predictions and a small effect in Study 3's (0.247) high purchase involvement predictions. Data quantity was not a significant factor for personality prediction accuracy.

Higher detailed data significantly increased purchase behavior prediction inaccuracy in studies 2a, 2b, and 3. High detail customer data (e.g., iTunes purchase records, Facebook detail data) significantly increased purchase behavior inaccuracy in both high and low purchase involvement contexts. Effect sizes ranged from small effects in Study 3 (0.252) and Study 2s (0.322) to a moderate effect in Study 2b (0.598). This is a surprising result, as the detail of the data should theoretically provide more information to respondents that should in turn improve prediction accuracy. Data detail was not a significant factor in personality predictions accuracy.

Social media content had moderate effects in Study 1 (0.588) and Study 3 (0.637), which reduced personality prediction inaccuracy significantly over transaction content. Data content was not a factor for purchase behavior predictions.

Data duality did not have any significant effects on prediction inaccuracy in any of the four experiments. Thus, dual source data performed as well as single source data when predicting both personality and future purchase behavior in terms of accuracy. The complementary aspects of merging social media and transaction data may still prove useful in other prediction tasks, but data duality was not a significant factor for accurately predicting personality and purchase behavior.

These accuracy results support Proposition 1, which states that data fit factors contribute to prediction value depending on the specific prediction task. Social media content (e.g., Facebook data) outperforms transaction content in terms of accurately predicting personality. High quantity and low detail data (e.g., credit card statements) increases prediction accuracy for purchase behavior predictions.

Social media data seemed to provide more arithmetically consistent personality predictions versus transaction data in Study 1, although this was not supported by Study 3's results. In all other cases, the four data fit factors had no apparent impact on prediction consistency. Thus, while prediction consistency is a desirable outcome that

partly defines the customer insight value, the data fit factors tested in these experiments do not contribute to either personality or purchase behavior prediction consistency.

Prediction experience did not have a significant impact on prediction accuracy. Thus, these results do not support Proposition 2's contention that prediction experience positively impact prediction accuracy. Perhaps if respondents had more prediction experience (i.e. add additional prediction tasks), or if respondents received feedback on the accuracy of their predictions, prediction experience might have more of a contribution to customer insight value.

3.5. Implications and Conclusions

The following paragraphs outline the major implications of this paper's findings for academic research and managerial practice. The section then details research limitations, potential future research avenues, and concludes with a summary of the theoretical and empirical contributions.

3.5.1. Research Implications

There are several important theoretical and empirical implications for academic research into customer surveillance and market intelligence. This paper also introduces a unique method of using experiments to predict consumer behavior that can be used in a variety of research settings.

This paper has three main theoretical implications for academic research. First, customer surveillance researchers need to consider customer surveillance from both the brand and the customer perspectives in order to fully evaluate market intelligence strategies. Brands require market intelligence to remain competitive in the marketplace because it enables innovation and improvement of products and services in line with customers' needs. If customers perceive a personal privacy threat due to customer surveillance activities, brands risk harming customer relationships. Thus, brands need to temper their desire for customer data and carefully consider the efficiency and effectiveness of customer surveillance activities. Scholars interested in studying

customer surveillance from a marketing, information systems, or public policy perspective need to better understand both the customer relationship with a brand and also the customer motivations to disclose their personal data.

Second, this paper proposes a framework for structuring market intelligence resources using surveillance prompts to increase the efficiency of customer surveillance. Surveillance prompts structure market intelligence resources so that customer data are collected for specific purposes (i.e. to answer the surveillance prompt), thus limiting the amount of customer data needed to obtain customer insights. Scholars can use this framework to evaluate market intelligence and customer surveillance strategies to, for example, explore methods of increasing the usefulness of customer data in predicting customer behavior.

Third, this paper proposes a model of customer insight value that can increase the effectiveness of customer surveillance activities by selecting customer data sources that more accurately and consistently predict a desired customer insight. The model evaluates customer data sources by assessing how well they fit the desired customer insight (Proposition 1). The theoretical contribution of prediction experience was not supported by empirical evidence (Proposition 2). Scholars can use this basic model to investigate additional data fit factors or other customer insights to further improve customer data effectiveness, thus narrowing the scope of customer surveillance needed.

From an empirical analysis perspective, the results of the four experiments show that depending on the specific customer insight desired, different data fit factors (data quantity, detail, content, and duality) are significant indictors of prediction accuracy (see Table 3.9). For example, data content was a significant data fit factor for predicting personality, but it was not significant for predicting future purchase behavior. Thus, researchers seeking to determine prediction value of other customer insights (e.g. why/motivation, where/location, etc.) need to test all data fit factors.

Table 3.9 Summary of Significant Prediction Accuracy Factors

Prediction Task	Data Fit Factors				Prediction Experience
	Quantity	Detail	Content	Duality	
Personality	No	No	Yes	No	No
Low purchase involvement behavior	Yes	Yes	No	No	Not tested
High purchase involvement behavior	Mixed	Yes	No	No	No

From a methodology perspective, this paper introduces the prediction experiment method. In traditional experiments, groups of respondents are manipulated or treated, and then the effect of the manipulation is statistically measured to determine causality (Creswell 2009). In prediction experiments, groups of respondents are also manipulated or treated, but respondents are asked for their prediction based on the data they have observed. For example, in Study 1, respondents observed data in one of eight data conditions, and then were asked to predict the personality of the individual whose data they had just observed. Personality prediction inaccuracy was measured by comparing how close they were to a friends and family comparison score. Both traditional and prediction experiments utilize between group comparisons to determine main and interaction effects of various variables. Researchers can use prediction experiments to, for example, explore the effectiveness of types of observed data.

3.5.2. Practical Implications

Marketers need to carefully consider their customer surveillance strategy to prevent potential damage to customer relationships. Using surveillance prompts to structure market intelligence resources and evaluating potential sources of customer data may reduce the need for extensive and obtrusive customer surveillance. Moreover, experimental evidence shows how the choice of customer data can impact the prediction accuracy and consistency of customer insights.

Data content was a significant factor that had a moderate effect on personality prediction accuracy. Facebook data performed on average 0.613 standard deviations better than transaction data in terms of personality prediction accuracy. Managers could

apply this finding, for example, by micro-targeting customers to specifically appeal to personality groups (e.g., the product's value for money could be highlighted for customers that are high economizers), or by tailoring customer services to meet specific personality traits (e.g., providing additional remote or home-visit services for customers that are highly home-oriented). Social media data have immense potential value for brands to discover many customer insights that have been difficult to predict using only transaction data (e.g., customer personality, purchase motivation, and brand usage). But social media data sources are often non-parametric or unstructured in contrast to parametric transaction or survey data, thus making analysis difficult with current technology (Halevy, Norvig, & Pereira 2009). Moreover, social media data are often public and easily accessible, but firms need to be aware of ethical considerations as they capture this data to reduce the potential negative impact on customer relationships (Boyd & Crawford 2011; Turow 2008).

Data quantity was a significant factor that increased the prediction accuracy of future purchase behavior that had a small effect on average (0.487 standard deviations). Moreover, results point to the small effect on average of data detail (0.391) that decreased future purchase behavior prediction accuracy. Thus brands, particularly low purchase involvement brands, should invest in customer data sources that are not necessarily detailed, but that capture a high quantity of data, such as credit card data, to predict future purchase behavior.

Since the data fit factors' results for personality and future purchase behavior are so different, marketers need to test potential data sources using prediction experiments to understand the potential prediction value of other customer insights. Using this knowledge of customer data sources and applying the surveillance prompt framework, marketers can gain more valuable customer insights with less customer surveillance.

3.5.3. Limitations and Future Research Directions

The following paragraphs outline several limitations of the research presented above along with new research directions that seek to address some of these limitations.

Then they discuss customer data issues, prediction concerns, method limitations, and other customer surveillance issues.

Because of financial, time, and logistical constraints, the customer data used in the experiments was collected from one individual. Additionally, data used in the experiments came from three sources (credit card statements, iTunes transaction records, Facebook data) over a short time period. Thus, even though the most of the empirical conclusions have been tested in more than one experiment, future study is needed to show the findings apply in other contexts. For example, future research might involve a more diverse set of individuals, or other varieties of personal data (e.g., more detailed retail transaction data, loyalty program records, other social media data). The data used in the experiments was collected from relatively short time periods (credit card: one month; iTunes: three months; Facebook: static screenshot), thus future studies could use panel customer data that may potentially provide more accurate and consistent predictions of various customer insights.

The experiments were also limited to predicting two forms of customer insights: customer personality (who) and future purchase behavior (what). Future research could examine other customer insight predictions using the same prediction experimental method, such as for example purchase motivation (why), location (where), preferred payment methods (how), purchase frequency (when), or willingness to pay (outcome). The results of these might provide much value for brands better using market intelligence resources. Prediction experience did not have a significant effect but future research could add more prediction task iterations or provide external feedback to examine the impact of perceptual learning on prediction.

As human respondents were used to make predictions using customer data, the method is limited to the mental capacity of individual respondents. Future research could examine what respondent attributes promote more accurate predictions. Furthermore, using the theoretical frameworks and empirical findings reported above, algorithms could be researched and written to recreate these experiments and remove the human dimension from customer insight prediction.

Customer surveillance is needed to ensure the competitiveness of a brand's products and services, but also should be limited in scope to preserve customer relationships with a brand. To further inform the selection of customer data sources, additional research needs to examine how customers respond to various kinds of customer surveillance activities, as some types of customer data might be seen as more sensitive than others. For example, some customers may perceive public social media data as more private than transaction data collected at the point of purchase. Thus, understanding customer surveillance attitudes and preferences are important to better satisfying customer needs and creating stronger customer relationships.

Brands need to understand and evaluate the ethical, reputational, customer relationship, legal, and other risks that underscore customer surveillance. The findings described above point to the benefit of collecting and analyzing public social media data to predict customer personality, but brands need to understand the ethical implications and risks before conducting social media surveillance. Future research into the ethics of customer surveillance may reveal important implications for management practice and public policy.

3.5.4. Concluding Thoughts

Customer relationships can be damaged if customers perceive a privacy threat due to a brand's customer surveillance activities. Customer surveillance collects and captures customer data that make up a brand's market intelligence resources, which aid the competitiveness of a brand's products and services. This paper introduces the surveillance prompts framework (who, what, where, when, why, how, and outcome) that structures market intelligence resources to provide firms with the ability to narrow the scope of customer surveillance. Furthermore, this paper also proposes a model of customer insight value that seeks to evaluate how well customer data sources can accurately and consistently predict specific customer insights.

Then, through a series of four experiments, this paper empirically explores eight different sets of customer data for their effectiveness in predicting customer personality and future purchase behavior. The findings include the benefit of social media

(Facebook) data in more accurately predicting customer personality, and high quantity, low detail (credit card) data in more accurately predicting future purchase behavior.

Brands can conduct efficient and effective customer surveillance by applying the surveillance prompt framework and evaluating potential customer data sources on the value of their predicted customer insights. The resulting market intelligence strategy allows product and service innovation and improvement while being sensitive to customer privacy and thus preserving customer relationships.

Chapter 4.

Conclusions

Customer surveillance is pervasive in offline and online marketplaces (Andrejevic 2007; Turow 2008). Yet, there has been little marketing or management research on customer surveillance activities, their impact on customers, and the management of these activities. This dissertation sought to address these unresearched topics through two papers (i.e., Chapters 2 and 3). The following paragraphs detail the specific contributions of each paper.

Chapter 2 investigated customer reactions to customer surveillance activities and found that some individuals generally process these experiences cognitively and some others automatically. The cognitive responses could be partly explained by the cognitive thought process suggested by the privacy calculus concept (Culnan & Bies 2003), but this does not explain automatic reactions. Using a personal concerns perspective (Baumgartner 2002), specifically consumer privacy and value concerns, Chapter 2 proposes attitudes towards customer surveillance that cognitively and automatically impact individuals' reactions to customer surveillance activities. For example, interview informants that were very concerned with either consumer privacy (i.e., protectionist archetype) or value (i.e., capitalist archetype) react to personal data requests automatically by either refusing to disclose due to privacy costs or disclosing to seek value, respectively. These attitudes can impact how an individual feels, thinks, or acts toward a brand, thus there are important managerial implications for how to target and respond to customers depending on their attitudes toward customer surveillance.

Chapter 3 examined customer surveillance from a strategic management perspective. It finds that brands need to temper their drive to obtain market intelligence through extensive customer surveillance in order to protect customer relationships. In

light of this, Chapter 3 proposes the surveillance prompt framework and a method of critically analyzing customer insight value from customer data sources. By using these, brands can efficiently and effective gain market intelligence with less customer surveillance, thus reducing customer relationship risks. Four experiments showed the utility of evaluating predicted customer insights that resulted in customer data source choice implications for managers.

This dissertation's focus on customer surveillance advances and enriches the surveillance, marketing, information systems, management, psychology, and sociology literatures. However, there are many more customer surveillance issues, questions, and problems that can be solved by research into this topic. Customer surveillance can provide individuals with outstanding products and services, if conducted in a manner that is sensitive to their concerns.

References

Aarts, H., & Dijksterhuis, A. P. (2000). The automatic activation of goal-directed behaviour: The case of travel habit. *Journal of Environmental Psychology*, *20*(1), 75-82.

Aarts, H., Verplanken, B., & Knippenberg, A. (1998). Predicting behavior from actions in the past: Repeated decision making or a matter of habit? *Journal of Applied Social Psychology*, *28*(15), 1355-1374.

Ailawadi, K. L., Neslin, S. A., & Gedenk, K. (2001). Pursuing the value-conscious consumer: store brands versus national brand promotions. *Journal of Marketing*, *65*(1), 71-89.

Ajzen, I. (2011). The theory of planned behaviour: reactions and reflections. *Psychology & Health*, *26*(9), 1113-1127.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological bulletin*, *84*(5), 888-918.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3).

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence, KS: University of Kansas.

Arnold, S. J., & Fischer, E. (1994). Hermeneutics and consumer research. *Journal of Consumer Research*, 21(1), 55-70.

Arnould, E., Price, L., & Moisio, R. (2006). Making contents matter: selecting research contexts for theoretical insights. In Belk, R., *Handbook of Qualitative Research Methods in Marketing*. Cheltenham, UK: Edward Egar Publishing Ltd.

Bagozzi, R. P. (1975). Marketing as exchange. *Journal of Marketing*, *39*(4), 32-39.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9).

Bartko, J. J. (1976). On various intraclass correlation reliability coefficients. *Psychological bulletin*, *83*(5), 762-765.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. Cambridge, UK: Polity.

Baumgartner, H. (2002). Toward a personology of the consumer. *Journal of Consumer Research*, *29*(2), 286-292.

Baumgartner, H., & Steenkamp, J. B. E. (1996). Exploratory consumer buying behavior: Conceptualization and measurement. *International Journal of Research in Marketing*, *13*(2), 121-137.

Bennett, C. J. (2008). *The privacy advocates*. Cambridge, MA: The MIT Press.

Berry, M. J., & Linoff, G. S. (2004). *Data mining techniques: for marketing, sales, and customer relationship management*. Indianapolis: Wiley Publishing.

Bisdikian, C., Branch, J., Leung, K. K., & Young, R. I. (2009). A letter soup for the quality of information in sensor networks. In the proceedings of *IEEE International Conference on Pervasive Computing and Communications 2009*, 1-6.

Blattberg, R. C., & Neslin, S. A. (1990). *Sales promotion: Concepts, methods, and strategies*. Englewood Cliffs, NJ: Prentice Hall.

Bollier, D., & Firestone, C. M. (2010). *The promise and peril of big data*. Washington, DC: Aspen Institute.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society, 15(5), 662-679.*

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.

Chandon, P., Wansink, B., & Laurent, G. (2000). A benefit congruency framework of sales promotion effectiveness. *The Journal of marketing*, *64*(4), 65-81.

Cohen, J. (1968). Weighted kappa: Nominal scale agreement provision for scaled disagreement or partial credit. *Psychological Bulletin*, *70*(4), 213-220.

Cohen, J. (1992). A power primer. *Psychological bulletin*, *112*(1), 155-159.

Craven, J. B. (1976). Personhood: The Right to Be Let Alone. *Duke Law Journal*, *1976*(4), 699-720.

Creswell, J. W. (2009). *Qualitative inquiry and research design: Choosing among five approaches*. Los Angeles, CA: Sage.

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., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323-342.

Dane, E., & Pratt, M. G. (2007). Exploring intuition and its role in managerial decision making. *Academy of Management Review*, *32*(1), 33-54.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Donaldson, T., & Dunfee, T. W. (1999). *Ties that bind: A social contracts approach to business ethics*. Cambridge, MA: Harvard Business Press.

Edwards, K. (1990). The interplay of affect and cognition in attitude formation and change. *Journal of Personality and Social Psychology*, *59*(2), 202.

Ellison, G., & Ellison, S. F. (2009). Search, obfuscation, and price elasticities on the internet. *Econometrica*, *77*(2), 427-452.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI magazine*, *17*(3), 37-54.

Fitzsimons, G. M., Chartrand, T. L., & Fitzsimons, G. J. (2008). Automatic effects of brand exposure on motivated behavior: how apple makes you “think different”. *Journal of consumer research*, *35*(1), 21-35.

Folkes, V. S. (1988). Recent attribution research in consumer behavior: A review and new directions. *Journal of Consumer Research*, 548-565.

Fournier, S. (1998). Consumers and their brands: Developing relationship theory in consumer research. *Journal of Consumer Research*, *24*(4), 343-353.

Fournier, S., & Yao, J. L. (1997). Reviving brand loyalty: a reconceptualization within the framework of consumer-brand relationships. *International Journal of Research in Marketing*, *14*(5), 451-472.

Funder, D. C. (1995). On the accuracy of personality judgment: a realistic approach. *Psychological Review*, *102*(4), 652-670.

Funder, D. C., & Colvin, C. R. (1988). Friends and strangers: acquaintanceship, agreement, and the accuracy of personality judgment. *Journal of Personality and Social Psychology*, *55*(1), 149-158.

Gayathri, A. (2013). Apple consumer lawsuit thrown out after judge rules plaintiffs failed to prove 'economic injury'. *International Business Times*, November 28.

Gilbert, F. W., & Warren, W. E. (1995). Psychographic constructs and demographic segments. *Psychology & Marketing*, *12*(3), 223-237.

Gillham, B. (2005). *Research interviewing: The range of techniques.* Maidenhead, UK: Open University Press.

Glaser, B. G., & Strauss, A. L. (2009). *The Discovery of Grounded Theory: Strategies for qualitative research*. London, UK: Transaction Books.

Glazer, R. (1991). Marketing in an information-intensive environment: strategic implications of knowledge as an asset. *Journal of Marketing*, *55*(4), 1-19.

Godkin, E. L. (1880). Libel and its legal remedy. *Journal of Social Science*, *12*, 69-80.

Goodman, J. K., Cryder, C. E., & Cheema, A. (2013). Data collection in a flat world: The strengths and weaknesses of Mechanical Turk samples. *Journal of Behavioral Decision Making*, *26*(3), 213-224.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, 611-642.

Haggerty, K. D., & Gazso, A. (2002). The public politics of opinion research on surveillance and privacy. *Surveillance & Society*, *3*(2/3), 173-180.

Halevy, A., Norvig, P., & Pereira, F. (2009). The unreasonable effectiveness of data. *Intelligent Systems, IEEE*, *24*(2), 8-12.

Hall, C. C., Ariss, L., & Todorov, A. (2007). The illusion of knowledge: When more information reduces accuracy and increases confidence. *Organizational Behavior and Human Decision Processes*, *103*(2), 277-290.

Harter, J. K., Schmidt, F. L., & Hayes, T. L. (2002). Business-unit-level relationship between employee satisfaction, employee engagement, and business outcomes: a meta-analysis. *Journal of Applied Psychology*, *87*(2), 268-279.

Hassin, R. R., Bargh, J. A., & Zimerman, S. (2009). Automatic and flexible: The case of non-conscious goal pursuit. *Social cognition*, *27*(1), 20-36.

Hoch, S. J. (1988). Who do we know: Predicting the interests and opinions of the American consumer. *Journal of Consumer Research*, 315-324.

Holbrook, M. (1994). The nature of customer value: An axiology of services in the consumption experience. In R. Rust, & R. Oliver (Eds.), *Service quality: New directions in theory and practice,* 21-72. Thousand Oaks, CA: SAGE Publications, Inc.

Homer, P. M. (1995). Ad size as an indicator of perceived advertising costs and effort: The effects on memory and perceptions. *Journal of Advertising*, *24*(4), 1-12.

Hoyer, W. D. (1984). An examination of consumer decision making for a common repeat purchase product. *Journal of consumer research*, *11*(3), 822-829.

Hoyer, W. D., & Brown, S. P. (1990). Effects of brand awareness on choice for a common, repeat-purchase product. *Journal of consumer research*, 141-148.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, 19-33.

Inness, J. C. (1992). *Privacy, Intimacy, and Isolation.* New York, NY: *Oxford*.

Janiszewski, C. (1988). Preconscious processing effects: The independence of attitude formation and conscious thought. *Journal of consumer research*, 199-209.

Jaworski, B. J., & Kohli, A. K. (1993). Market orientation: antecedents and consequences. *The Journal of Marketing*, 53-70.

Kahneman, D. (2011). *Thinking, fast and slow*. Toronto, ON: Doubleday Canada.

Kahneman, D., & Tversky, A. (1973). On the psychology of prediction. *Psychological Review*, *80*(4), 237.

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, *54*(3), 241-251.

Kietzmann, J., & Angell, I. (2010). Panopticon revisited. *Communications of the ACM*, *53*(6), 135-138.

Kim, J., Lim, J. S., & Bhargava, M. (1998). The role of affect in attitude formation: A classical conditioning approach. *Journal of the Academy of Marketing Science*, *26*(2), 143-152.

Kobsa, A. (2007). Privacy-enhanced personalization. *Communications of the ACM*, *50*(8), 24-33.

Kohli, A. K., & Jaworski, B. J. (1990). Market orientation: the construct, research propositions, and managerial implications. *Journal of Marketing*, 1-18.

Kolar, D. W., Funder, D. C., & Colvin, C. R. (1996). Comparing the accuracy of personality judgments by the self and knowledgeable others. *Journal of Personality*, *64*(2), 311-337.

Kruglanski, A. W. (1989). The psychology of being" right": The problem of accuracy in social perception and cognition. *Psychological Bulletin*, *106*(3), 395-409.

Kuechler, W., & Vaishnavi, V. (2012). A framework for theory development in design science research: multiple perspectives. *Journal of the Association for Information systems*, *13*(6), 395-423.

Kwasny, M., Caine, K., Rogers, W. A., & Fisk, A. D. (2008, April). Privacy and technology: folk definitions and perspectives. In the Proceedings of *CHI'08 Extended Abstracts on Human Factors in Computing Systems*, 3291-3296.

Larson, J. H. & N. J. Bell. (1988). Need for Privacy and Its Effect Upon Interpersonal Attraction and Interaction. *Journal of Social and Clinical Psychology* 6, 1–10.

LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., & Kruschwitz, N. (2013). Big data, analytics and the path from insights to value. *MIT Sloan Management Review*, *52*(2), 21-31.

Lee, L., & Ariely, D. (2006). Shopping goals, goal concreteness, and conditional promotions. *Journal of Consumer Research*, *33*(1), 60-70.

Lichtenstein, D. R., Netemeyer, R. G., & Burton, S. (1995). Assessing the domain specificity of deal proneness: a field study. *Journal of Consumer Research*, *22*(3), 314-326.

Lyon, D. (2001). *Surveillance Society*. Buckingham, UK: Open University Press.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.

Maio, G., & Haddock, G. (2009). *The Psychology of Attitudes and Attitude Change*. London, UK: Sage.

Malhotra, N. K., Kim S. S., & Agarwal J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research* 15(4), 336-355.

Marshall, N. J. (1972). Privacy and environment. *Human Ecology*, *1*(2), 93-110.

McAfee, A., & Brynjolfsson, E. (2012). Big data: the management revolution. *Harvard Business Review*, *90*(10), 60-6.

McCombs, M. (2004). *Setting the agenda: The mass media and public opinion*. Cambridge, UK: Polity.

Millar, M. G., & Millar, K. U. (1990). Attitude change as a function of attitude type and argument type. *Journal of Personality and Social Psychology*, *59*(2), 217-228.

Milne, G. R., & Bahl, S. (2010). Are there differences between consumers' and marketers' privacy expectations? A segment-and technology-level analysis. *Journal of Public Policy & Marketing*, *29*(1), 138-149.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15-29.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, 20-38.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *The Journal of Marketing*, *58*(3), 20-38.

Newell, P. B. (1998). A cross-cultural comparison of privacy definitions and functions: A systems approach. *Journal of Environmental Psychology*, *18*(4), 357-371.

Petrov, A. A., & Anderson, J. R. (2005). The dynamics of scaling: a memory-based anchor model of category rating and absolute identification. *Psychological Review*, *112*(2), 383-416.

Petrov, A. A., Dosher, B. A., & Lu, Z. L. (2005). The dynamics of perceptual learning: an incremental reweighting model. *Psychological Review*, *112*(4), 715-743.

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.

Plangger, K., & Watson, R. (2015). Customer privacy, secrets, and surveillance: creating an effective foundation for insights. *Business Horizons*, forthcoming.

Posner, R. A. (1981). The economics of privacy. *The American economic review*, *71*(2), 405-409.

Puccinelli, N. M., Goodstein, R. C., Grewal, D., Price, R., Raghubir, P., & Stewart, D. (2009). Customer experience management in retailing: understanding the buying process. *Journal of Retailing*, *85*(1), 15-30.

Salanova, M., Agut, S., & Peiro, J. M. (2005). Linking organizational resources and work engagement to employee performance and customer loyalty: the mediation of service climate. *Journal of Applied Psychology*, *90*(6), 1217-1227.

Schneider, C. D. (1972). *Shame, Exposure, and Privacy.* New York: NY: WW Norton & Co Inc.

Shoemaker, P. J. (1996). Hardwired for news: Using biological and cultural evolution to explain the surveillance function. *Journal of Communication*, *46*(3), 32-47.

Shrout, P. E., & Fleiss, J. L. (1979). Intraclass correlations: uses in assessing rater reliability. *Psychological Bulletin*, *86*(2), 420-428.

Slater, S. F., & Narver, J. C. (1995). Market orientation and the learning organization. *Journal of Marketing*, 63-74.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, *20*(2), 167-196.

Solove, D. (2008). Understanding privacy. Cambridge, UK: Harvard Press.

Spitzer, R. L., Cohen, J., Fleiss, J. L., & Endicott, J. (1967). Quantification of agreement in psychiatric diagnosis: a new approach. *Archives of General Psychiatry*, *17*(1), 83-87.

Sweeney, J. C., & Soutar, G. N. (2001). Consumer perceived value: The development of a multiple item scale. *Journal of Retailing*, *77*(2), 203-220.

Thomsen, E. (1997). *OLAP solutions: building multidimensional information systems*. New York, NY: Wiley.

Turow, J. (2008). *Niche envy.* Cambridge, MA: MIT Press.

Uleman, J. S. (1999). Spontaneous versus intentional inferences in impression formation. *Dual-process Theories in Social Psychology*, 141-160.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220.

Watson, R. T. (2013). *Data management: databases and organizations (6th ed.)*. Athens, GA: eGreen Press.

Welch, E. (2005). *Shopping in the Renaissance: consumer cultures in Italy 1400-1600*. London, UK: Yale University Press.

Westin, A. (1967). *Privacy and freedom*. New York, NY: The Bodley Head Ltd.

Woodside, A. G., & Trappey, R. J. (1992). Finding out why customers shop your store and buy your brand: Automatic cognitive processing models of primary choice. *Journal of Advertising Research*.

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), 1.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, *26*(3), 135-174.

Yoon, S., & Vargas, P. T. (2010). Feeling happier when paying more: Dysfunctional counterfactual thinking in consumer affect. *Psychology & Marketing*, *27*(12), 1075-1100.