Available online at www.sciencedirect.com

ScienceDirect

Journal of Interactive Marketing 50 (2020) 32–44

JOURNAL OF INTERACTIVE MARKETING

www.elsevier.com/locate/intmar

Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance

Kirk Plangger *& Matteo Montecchi

King's Business School, King's College London, London, UK

Abstract

As interactive technologies become more pervasive, firms are increasingly conducting customer surveillance—the acquisition, usage, and storage of consumers' personal data—more covertly and with fewer resources. Privacy calculus—the rational decision to disclose personal data—has dominated the literature to explain rational or calculated reactions to customer surveillance, however, not all reactions can be explained by rational processes. This article advances our understanding of these reactions beyond the privacy calculus concept by proposing attitudes toward customer surveillance. Based on levels of consumer privacy and consumer value concerns, these attitudes are associated with four archetypes—pragmatists, protectionists, capitalists, and apathists. By understanding these attitudes, researchers and managers can gain insight into the diversity of consumers' concerns regarding both consumer privacy and consumer value in order to better explain observed marketplace behaviors.

Keywords: Customer surveillance; Consumer privacy; Consumer value; Personal concerns; Consumer attitudes; Privacy calculus

Introduction

As marketing embraces the science of analytics (Bauman and Lyon 2013; Moe and Ratchford 2018), marketing managers need to reflect on the impact of surveillance practices on their customers. Customer surveillance, which involves the acquisition, usage, or storage of customers' personal data (Plangger and Watson 2015), can be a source of competitive advantage by generating customer insights. These customer insights produce market intelligence—data on customers' needs, preferences, characteristics, behavior, attitudes, and other attributes—to influence, target, and manage customers, as well as to proactively respond to customers' needs (Holtrop et al. 2017; Kohli and Jaworski 1990; Wood and Ball 2013). Managers have a long history of using customer surveillance and market intelligence to gain a competitive edge and enjoy enhanced customer loyalty, satisfaction, and relationships (Jaworski and Kohli 1993). Marketing intelligence has become a central part of marketing operations for many firms across a wide variety of industries (Albrechtslund 2008; Deighton and Kornfeld 2009; Moe and Ratchford 2018). However, marketing managers also need to scrutinize the effects of surveillance investments on customers' attitudes, loyalty, and behavior in order to identify and mitigate negative outcomes.

Customers face tradeoffs between protecting their personal data and enjoying the benefits afforded by firms having access to their personal data (e.g., improved products, discounts, increased convenience, status rewards, etc.). To explain consumer reactions to customer surveillance, Culnan and Armstrong (1999) propose *privacy calculus* that clarifies how consumers rationally balance the benefits and costs of disclosing personal data. This rational approach has dominated the consumer privacy literature (c.f. Dinev, McConnell, and Smith 2015; Smith, Dinev, and Xu 2011); however, rationality can often be partial or limited in the context of information privacy (John, Acquisti, and Loewenstein 2011; Poddar, Mosteller, and Ellen 2009). This can be driven by situational and environmental cues including convenience, data requestor–discloser relationship, resource limitations, data sensitivity, and subjective or cultural norms (John, Acquisti, and Loewenstein

* Corresponding author at: King's Business School, King's College London, Bush House, 30 Aldwych, London WC2B 4BG, United Kingdom.
E-mail address: kirk.plangger@kcl.ac.uk (K. Plangger).

https://doi.org/10.1016/j.intmar.2019.10.004
1094-9968

2011; Poddar, Mosteller, and Ellen 2009). Furthermore, individuals often rely on heuristics to accelerate decisions and preserve cognitive resources (Kahneman 2011), which are also not accounted for in privacy calculus. This article proposes attitudes toward customer surveillance, which influences both rational and heuristic data disclosure decisions.

From a relationship perspective, firms are primarily concerned with serving and satisfying current customers, as well as attracting potential customers, rather than collecting personal data from them (Berry and Linoff 2004). Customer relationships, which are built on perceptions of integrity and honesty (Marshall 1972; Fournier 1998; Morgan and Hunt 1994), may wither if customer surveillance activities threaten customers' personal data privacy may result in firm-switching behavior. Thus, firms must temper the need for customer surveillance to protect these relationships while still gaining the data they need to remain competitive. Firms can achieve this balance by thinking strategically about customer surveillance instead of focusing on different surveillance tactics or technologies (Plangger and Watson 2015). Furthermore, firms also need to understand how customers feel, think, and intend to behave when facing surveillance tactics to build an optimal customer surveillance strategy.

Attitudes toward customer surveillance are based on individuals' personal concerns (Baumgartner 2002) regarding consumer privacy (Malhotra, Kim, and Agarwal 2004; Smith, Milberg, and Burke 1996) and consumer value (Ailawadi, Neslin, and Gedenk 2001; Lichtenstein, Netemeyer, and Burton 1990). These attitudes influence consumers' reactions to customer surveillance activities, including changes in consumption frequency, switching behavior, relative indifference, and changes in other attitudes. Based on literature insights, these attitudes are theoretically developed in the next section by defining their consequences, influences, and composition. Then, interviews shed light on how these attitudes shape behaviors and result in four attitude archetypes. Next, a survey study finds associations with a number of cultural and psychological factors, as well as confirming behavioral insights gained from the interviews. The article closes by discussing practical implications and suggesting a research agenda.

Theory Development

Surveillance and Privacy

Surveillance is pervasive in modern society as it touches some part of daily life for most individuals, whether they are aware of it or not (Lyon 2007; Wood and Ball 2013). Surveillance is the "focused, systematic, and routine attention to personal details for the purposes of influence, management, protection, or direction" (Lyon 2007, p 14). Connected to surveillance is the concept of information privacy that involves an individual's ability to control the use, release, collection, storage, and access to their personal data (Malhotra, Kim, and Agarwal 2004). The more private an individual, firm, or organization is, the more others desire surveillance of that individual (Lyon 2007). Because of this link between information privacy and surveillance, surveillance often has a negative connotation related to the privacy costs and security risks borne by the surveillance targets despite the potential benefits that may accrue from surveillance (Albrechtslund 2008).

Firms need to acquire data about their customers to remain competitive, evaluate marketing strategies, innovate market offerings, and obtain consumer insights (Albrechtslund 2008; Deighton and Kornfeld 2009; Holtrop et al. 2017). A customer surveillance strategy enables customer data acquisition though the deployment of surveillance tactics. Some common tactics involve, for example, tracking transactions through loyalty programs (Blattberg and Deighton 1991; Turow 2008), observing clickstreams or digital behavioral data (Bucklin and Sismeiro 2009, 2003), audio or video recording consumer interactions (Lyon 2007; Turow 2008), and applying location-based technologies (e.g., GPS, RfID) to monitor consumers or products (Junglas and Watson 2008).

However, customer surveillance also risks customer relationships and might even breed mistrust among consumers (Mosteller and Poddar 2017; Turow 2008). Customer relationships with firms are fragile and are built on customers' perceptions of a firm's integrity and honesty (Morgan and Hunt 1994). If customers discover that their data are misused or insecurely stored, customer relationships may be damaged, and their attitudes toward that firm may be negatively impacted (Krafft, Arden, and Verhoef 2017; Shmargad and Watts 2016; Andrejevic 2007). Thus, marketing managers and researchers need to understand consumers' attitudes toward customer surveillance and the influence of those attitudes on behaviors.

Responses to Customer Surveillance

As attitudes are cognitive structures that shape thoughts, feelings, and intended actions (Ajzen 2011; Ajzen and Fishbein 1977), attitudes toward customer surveillance influence individuals' behavior when faced with personal data disclosure decisions along with other contextual factors. Individuals perceive customer surveillance both independently and collectively with others through media and other interactions (McCombs 2004). However, when perceptions are shared, individuals often have very different reactions to personal data threats (Xu et al. 2011). Consider two consumers who read the same blog exposing a firm's unknown customer surveillance activities resulting in a similar perception of the firm's activities; however, they have different attitudes toward customer surveillance. The consumer with a relatively more negative attitude is more likely to terminate the relationship with the offending firm compared to the other consumer. While having similar shared perceptions is useful to understand the attitude's effect, this effect likely applies to when perceptions are different.

A negative attitude toward customer surveillance does not always translate into negative behavior directed to firms that conduct the surveillance. While intentions commitment can explain part of this discrepancy (Ajzen and Fishbein 1977), the Theory of Planned Behavior (Ajzen 2011) describes how

intentions capture motivational influences—attitudes, subjective norms, perceived control, past behavior—that influence actual behavior. However, there are contextual factors that also influence actual behavior (e.g., time, money, skills, opportunity, perceived control; Ajzen 2011). Thus, even when an individual intends to avoid customer surveillance due to motivational influences, contextual factors may upset this intention. While contextual factors are important to predict actual behavior (Smith, Dinev, and Xu 2011; Xu et al. 2011), the influence of attitudes toward customer surveillance has not been previously examined.

Beyond Privacy Calculus

Dominating the privacy literature (Dinev, McConnell, and Smith 2015; Smith, Dinev, and Xu 2011), privacy calculus describes a rational analysis that balances the benefits and costs of disclosing personal data to a firm (Culnan and Armstrong 1999). When individuals evaluate a disclosure decision's utility (u), they will consider the perceived value of the benefits that accrue from the exchange (v) minus any monetary price (p), search costs (s), and the perceived harm of sacrificing privacy (h). Formally:

$$u = v - (p + s + h)$$

By increasing search costs (s), individuals may find market offerings that either provide additional value (v), reduced prices (p), or decreased perceived harm (h). Alternatively, by sacrificing more of their privacy (h), individuals may access personalized offers of higher net value ($v - p$) by tailoring these offers using the data disclosed while reducing search costs (s). Using privacy calculus, these complex tradeoffs are carefully considered and thus require considerable cognitive resources.

However, the privacy calculus concept does not consider the possibility of decisions made using partially rational or heuristic decision processes. Especially when cognitively overloaded or making unimportant decisions, individuals routinely preserve cognitive resources and employ heuristics developed from past experiences and attitudes (Bargh et al. 2001; Kahneman 2011). Thus, for some consumers, other nonconscious factors may have greater influence than a rational privacy calculus analysis when making disclosure decisions (John, Acquisti, and Loewenstein 2011).

The personal concerns of consumer privacy and value are two salient factors when individuals face disclosure decisions. Personal concerns refer to "the goals that people pursue in their lives and the effects that these goals have on personal outcomes" (Baumgartner 2002: 287). These concerns are highly idiographic and contextualized, and they influence consumer behavior, attitudes, and decisions. As they are derived from internal goals, personal concerns can range from a very salient concern that directs consumption decisions in ways to achieve that goal to a very low concern that is likely unimportant with regard to decision-making (Baumgartner 2002). Specifically, *consumer privacy concern* involves a consumer's level of anxiety about the potential personal privacy costs associated with consumption (h), while *consumer value concern* involves a consumer's motivation to seek additional benefits (v) and reduce costs that accrue from consumption ($p + s$). The relative salience between these personal concerns forms attitudes toward customer surveillance that can influence decisions to disclose data.

Consumer Privacy Concern

Consumer privacy concern refers to the anxiety individuals experience regarding their personal data in the consumption context (Smith, Dinev, and Xu 2011). Although privacy in cultural (Mehta and Belk 1991) and sociodemographic (Hill and Stamey 1990) contexts may differ, this article defines privacy as an outcome of an individual's desire to withhold personal data from others (Larson and Bell 1988). Individuals perceive personal data as private when those data are central to their identity (e.g., birth date, sexual orientation, relationship status, address, credit card, and health data), or when there is a non-intimate relationship between the data discloser and the recipient (Marshall 1972). Consumers often have intimate relationships with firms (Fournier 1998); thus, they may feel that some data requested by these firms are not private. Privacy perceptions can be impacted by environmental cues that either induce or mitigate individuals' privacy concerns (John, Acquisti, and Loewenstein 2011). However, even though privacy perceptions can be manipulated, salient consumer privacy concerns can impact behavior by forming decision heuristics (Phelps, Nowak, and Ferrell 2000).

Consumers differ with regard to privacy concern reflecting their anxieties that firms will not be faithful to the implicit contract when exchanging their data for benefits (Phelps, Nowak, and Ferrell 2000). Those who are extremely concerned with privacy form decision heuristics to protect their privacy and will likely reject firms' data requests quickly. Alternatively, those who are less concerned with privacy will likely not have a privacy protecting heuristic and could spend more time considering data requests. Consumers who have some concern for their privacy will likely rationally weigh consumer privacy concerns with other contextual factors to make a disclosure decision similar to the privacy calculus concept. Thus, the salience level of individuals' consumer privacy concern partly influences their attitude toward customer surveillance.

Consumer Value Concern

Consumer value concern refers to the anxiety consumers experience obtaining increased benefits and reduced costs from their consumption (Ailawadi, Neslin, and Gedenk 2001; Lichtenstein, Netemeyer, and Burton 1990). Consumer value involves an assessment of a product or service's ability to achieve value goals weighed against perceived sacrifices (Kim and Niehm 2009; Woodruff 1997; Zeithaml 1988) through the provision of utilitarian (e.g., discounts on price, added convenience, more freebies) and hedonic (e.g., higher status level, access to exclusive information, added fun or adventure) benefits (Babin, Darden, and Griffin 1994; Shankar et al. 2016; Sherry Jr 1990). This perceived value has functional (i.e., how

well a product performs), social (i.e., how it signals status), emotional (i.e., how it generates affect), epistemic (i.e., how it satisfies the need for knowledge), and conditional (i.e., how it is relevant to the situation) categories of expected utility (Sheth, Newman, and Gross 1991). Network effects (e.g., word-of-mouth, observational learning; Marchand and Hennig-Thurau 2013) also affect consumer value. Value perceptions have been successfully controlled in past experiments by manipulating reference prices (Alford and Biswas 2002), goal concreteness (Lee and Ariely 2006), and positive affect (Yoon and Vargas 2010). These studies find that a salient consumer value concern can affect consumers' choices through the activation of heuristic mechanisms.

Individuals differ with regard to their value concerns and show varying levels of anxiety for obtaining additional value within a consumption context (Ailawadi, Neslin, and Gedenk 2001; Babin, Darden, and Griffin 1994; Shankar et al. 2016). Those individuals with highly salient value concern would likely form a strong decision heuristic to seek out additional benefits offered from personal data disclosure, whereas those that are less concerned would not likely form this heuristic. Outside of these extremes, consumers who have some degree of concern for consumer value would likely engage in a rational process to decide whether to disclose their personal data.

The marketing literature understands many aspects of consumer value concern from the perspective of sales transactions; however, outside this specific (albeit large and important) context, there has been little research. From the perspective of personal data disclosure, privacy researchers have largely discounted the benefits of customer surveillance as being relatively small compared to the personal privacy and data security costs (c.f., Turow 2008; Andrejevic 2007; Smith, Dinev, and Xu 2011). Consumer value concern partly influences consumers' decision to disclose data, thus forming an integral part of their attitudes toward customer surveillance.

Attitudes Toward Customer Surveillance

Taken together, the personal concerns for consumer privacy and value form attitudes toward customer surveillance that reflect how individuals think, feel, and intend to act in response to customer surveillance situations. The Stimulus–Organism–Response framework (Davis and Luthans 1980; Poddar, Mosteller, and Ellen 2009; Wang et al. 2019) illustrates the impact that these attitudes have on disclosure decisions. Individuals faced with disclosure decisions (i.e., stimulus) mentally process them (i.e., organism) in a way that influences how those individuals decide to act (i.e., response). Considering only the organism and its mental processes, attitudes toward customer surveillance provide a lens for individuals to interpret disclosure decisions before them. Consistent with the privacy calculus formula introduced above, these attitudes influence perceptions of net value ($v - p$) and privacy cost (h) of disclosing data regardless of specific contexts. However, there are remaining research questions about how these attitudes work in practice to influence decisions that the next section will explore using interviews and a survey:

(1) How do consumer privacy and value concerns influence disclosure behavior?
(2) What other factors influence perceptions of customer surveillance?
(3) What strategies are employed by individuals to manage customer surveillance?
(4) How do individuals make decisions to disclose personal data?

Empirical Explorations

Interview Study

The interview study further develops the understanding of attitudes toward customer surveillance by exploring the four research questions posed above. It reports the results of 26 semi-structured interviews that investigate individuals' attitudes toward customer surveillance and their influence on disclosure decisions. Interviews are a common method that allows informants to offer deep explanations of concepts that are poorly understood (Arnold and Fischer 1994; Creswell 2009), such as these attitudes. An interview worksheet guided the interviews to direct informants to four customer surveillance topics without referring to "surveillance." Interviews began with privacy and personal data definitions to qualify informants' responses. Next, they explored informants' views on, and experiences with, customer surveillance (e.g., loyalty cards in their wallets). Informants reported a variety of positive and negative experiences with data requests, which were used to examine their feelings, thoughts, and behaviors. They were then asked to offer advice for both a friend and a firm on how to manage data requests. Finally, interviews closed by recording demographics to aid informant comparison.

The interviews were recorded, transcribed, and then analyzed using an inductive approach with the following steps: (1) open coding of the first set of 10 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 categories; and (4) hermeneutic interpretation of the findings (Arnold and Fischer 1994). Privacy and value concerns were coded to aid the mapping of informants into archetypes. Some informants exhibited high degrees of privacy concern in a general or government surveillance context, but this did not always translate into consumer privacy concern. While there is a possibility of a single researcher coding bias, the authors attempted to minimize the possible impact of such bias on the analysis through discussions with several privacy scholars about coding assessments and theme conclusions.

Informants were invited to participate in interviews across various demographic categories (e.g., gender, age, culture, and occupation) to provide a broad range of perspectives on customer surveillance. They were asked to suggest other

potential informants using a snowball sampling method until theoretical saturation, and no new insights emerged from the informants' responses (Creswell 2009). All informant interviews took place either via Skype or face-to-face in Canada or the United Kingdom. Theoretical saturation became evident after 22 interviewers (i.e., at least two individuals were mapped into archetypes); however, 4 additional interviews were also performed, as they were already scheduled. Interviews lasted an average of 24 minutes. Table 1 reports informants' gender, occupation industry, age, and nationality.

The interview findings have been organized into four attitude archetypes depending on the exhibited salience of the personal concerns for consumer privacy and value: protectionists, capitalists, pragmatists, and apathists (see Fig. 1). *Protectionists* are highly concerned with consumer privacy but are not concerned with consumer value. Thus, they are likely to quickly refuse personal data requests even when offered valuable benefits due to the risk to their personal data. *Capitalists* are very concerned with seeking out consumer value without much concern for their consumer privacy, so they are more likely to quickly disclose personal data if there is a clear benefit to them. *Pragmatists* have high personal concerns for both consumer privacy and consumer value, so they are more likely to rationally consider personal data requests. Finally, *apathists* report not having personal concern for either consumer privacy or value, so their disclosure decisions are likely to be influenced by other factors. The next four sub-sections examine evidence from the informants' responses to deepen the understanding of the archetypes.

Table 1
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 Arabian
X	Female	Early 30s	Student	German
Y	Female	Early 30s	Consulting	Korean
Z	Male	Early 30s	Education	Turkish

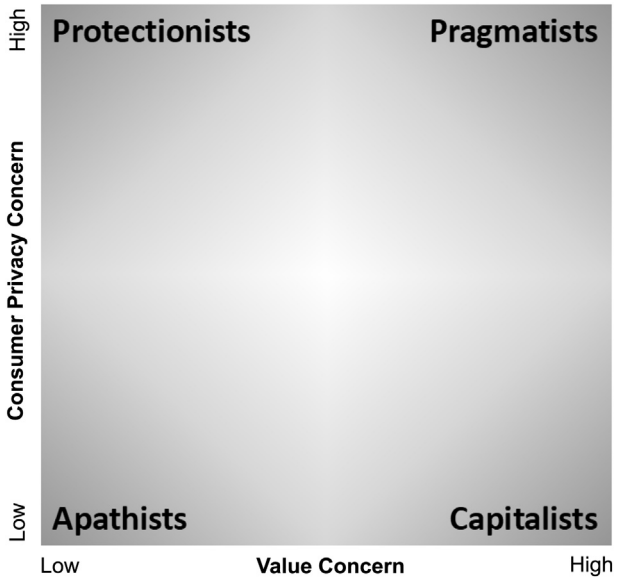

Fig. 1. Archetypes of attitudes toward customer surveillance.

Protectionists

Protectionist informants exhibit a high consumer privacy concern and a relatively low value concern that negatively impact disclosure behaviors including, in some extreme cases, the rejection of digital interactions (Milne and Culnan 2004). Turning first to consumer privacy concern, Informant N highlights collection and awareness concerns in her comment, "I wouldn't like it if [firms] had all my info and they knew everything about me before I step through the door." 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."

Informant R is also careful about whom he provides with his personal data; when advising a hypothetical friend, he said:

> 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.

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

Many protectionist informants claim that there are few customer surveillance benefits that they perceive as worthwhile. For example, Informant G was adamant in her comment about the benefits of disclosure:

> 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.

While this informant feels very strongly about the lack of value for her, some other protectionists are less extreme in their responses. Informant Q admits to considering some benefits but still relies on a "do not disclose" heuristic. She claims, "[firms] only need an email and birthdate to send the freebies. [They] don't need anything else." Thus, she admits to accepting "freebies" but is wary of how free a "freebie" is in terms of privacy cost. In sum, protectionists are characterized by their lack of consumer value concern and highly salient concern for consumer privacy. These privacy concerns significantly undermine protectionists' motivation to seek additional value through the data disclosure, thus may lead to heuristic-based decisions.

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 to obtain additional value. For example, Informant E explains how she sees her personal data:

> I drive a [SUV] 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, [it still] 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.

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

Capitalists are motivated by the opportunity to increase consumer value, and this motivation offsets their privacy concerns. They are primarily driven to maximize functional value (e.g., reduce price, get a better deal, access to sales promotions), although the emotional (e.g., feel good) and conditional value (e.g., special occasion) dimensions also play a role in their decision to disclose. Informant W reflects this when she talks about point cards: "I really need that card because the points there are very helpful." Later she elaborates on the consumer value she receives from a loyalty card: "I will get more opportunities, like when the new [fashion] collection comes, [the firm] will have champagne parties or something, and they have sales"; "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 functional, emotional, and conditional consumer value she gets outweighs any consumer privacy concern she may have. Regarding her reasons for disclosing personal data, Informant K says, "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 for this lack of concern for consumer privacy:

> 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.

She theorizes that firms are collecting this data for their mutual benefit to improve the goods she buys in functional ways.

Many capitalist informants exhibit high degrees of trust in firms, as Informant E states: "I don't think that anyone really wants personal information so that they can bring you harm." Informant C reveals that he trusts firms more than government when he said, "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 by saying, "I would probably say if you are going to overshare, stick with trusted companies that you know. It's probably going to be okay." Informant B explains that there are implicit firm-consumer contracts 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… 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.

Outside of the contract metaphor, other capitalist informants show their high levels of trust in firms. 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.

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

Many capitalist informants are aware of customer surveillance in their lives, but their trust in firms may weaken their concern for consumer privacy. Informant T reports low privacy concerns, as she believes that personal data requests are not about privacy concerns:

> 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].

For her, as well as other capitalists, disclosure requests are turned down not for consumer privacy reasons but for the lack of explicit utility or irritation at the lack of convenience.

Many capitalists claim that they wish that customer surveillance activities were even more pervasive, as they think it would make the consumption experience easier. Informant K states, "I like [Internet] cookies because I love to get targeted, 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 [firms] 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'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.

These informants report that they prefer to disclose personal data to increase convenience in their lives or obtain some other explicit hedonic or utilitarian benefits. As capitalists are characterized by a very salient concern for value without much concern for consumer privacy, they form a bias that directs their decision making when faced with disclosure requests. In extreme cases, this can result in a pro-value heuristic that leads to faster decisions to entertain disclosure requests to gain additional value.

Pragmatists

Pragmatists are characterized by high concerns for both consumer privacy and consumer value. These informants carefully evaluate each instance of customer surveillance they encounter to assess consumer privacy risks and potential consumer value. 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 [them] your information and whether or not what they give you back in exchange for your information is something you value. So, you are selling your information. It is a give and take.

For him, personal data are commodities that need protection and are shared only for valuable benefits. This is typical for pragmatists, as they carefully weigh the benefits and the risks of disclosing personal data.

However, consumer value is not the only aspect that pragmatists consider when deciding to provide data, as Informant X 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.

Thus, she values her personal data and filters firms based on their reputation. Like protectionists, pragmatists consider a firm's characteristics and their social relationship to that firm when deciding to disclose their data.

Pragmatists are characterized by a high consumer value concern that competes with their privacy concern, as Informant H reports:

> [Firms having access to my data is] useful to me in a sense. I feel I like this brand… [is] actually using [my] information in a meaningful way… [But] just because I shop once on a website or [go] 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.

This informant recognizes that there are valuable benefits, especially with firms he uses frequently, but he is also worried about his personal data being kept by firms that he does not frequent. As such, he is a typical pragmatist, since they require clear evidence of potential value in exchange for their data, like capitalists. Although their assessment of value is often based on the functional dimension, emotional and social dimensions also play a role in influencing pragmatists' overall perception of consumer value. The complex relationship between the competing high personal concerns for consumer privacy and consumer value forces pragmatists to rationally consider cases of customer surveillance.

Apathists

Apathists, or apathetic consumers, are characterized by a low concern for both consumer privacy and consumer value. Although there were just two informants that exhibited this archetype, they are essential to include, as they provide an important contrast to the other three archetypes. Because of their lack of consumer privacy concern, apathists apparently do not mind sharing their personal data. For example, Informant S repeatedly responded "No" or "No, I think I am fine with that" to questions asking whether he had a problem with retail firms, such as his local grocery store or Amazon, tracking his purchasing and shopping behavior. He elaborates:

> [Tracking] what I buy doesn't bother me, because it could help [the firm]. They want… to know if people are going to buy this much stuff, etc., and that could help them to know how much they should buy or produce [of that] stuff. Maybe it's because I may not buy stuff that I am afraid that other people would know, you know. I buy other stuff… so I don't care.

Informant S is like many capitalist informants in his view of consumer privacy both in his view on the purpose of customer surveillance and in his claim 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 is a requirement of being part of modern society. These informants go on to describe the inconvenience or boredom of receiving data collection requests from firms, as well as a general lack of anxiety regarding customer surveillance. Thus, apathists have a relatively low concern for consumer privacy.

Turning now to the concern for consumer value, neither of the apathetic informants could quickly recall being part of any point or loyalty programs; however, after probing further, it was found that both were part a program: Informant S receives a free movie as a reward from the local cinema, while 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 avoid joining other loyalty programs because of some privacy fear, like protectionists. Thus, these apathetic informants are characterized as not seeking consumer value nor wanting to protect their privacy, which leads them not to rationally consider disclosure requests.

The following study show evidence that confirms the speed at which disclosure decisions are made do differ across the archetypes, as well as providing additional clarity on how behavioral, cultural, and psychological factors vary between archetypes.

Survey Study

The results of an online survey reveal not only additional depth into the four attitude archetypes in terms of behavioral, cultural, and psychographic differences, but also insights into cognitive processing variations. Conducted using the services of TurkPrime.com, the survey received 752 complete responses from English-speaking consumers (Americans = 89.1%, British = 4.9%, Canadians = 3.8%, others = 2.2%). However, after removing failed attention checks and non-unique IP addresses, 688 remained in the sample. The sample is slightly biased toward females (53.3%), relatively young with 68.2% under 35 years old and largely employed (67.4%) with 85.9% having some kind of post-secondary education. The vast majority of the sample identifies as white (72.4%) with 52.5% reporting that they make under US$40,000. These sociodemographic characteristics were not significant indicators of disclosure behavior or associated with the archetypes.

These archetypes are extreme theoretical individuals, thus they were produced from three-way splits of respondents' answers to Dinev and Hart's (2006) Internet privacy concern scale (mean = 5.04, median = 5.25, standard deviation = 1.53, alpha = 0.92) and Lichtenstein, Netemeyer, and Burton's (1990) value consciousness scale (mean = 5.84, median = 5.86, standard deviation = 0.78, alpha = 0.80). The middle third of respondents for each scale was removed from the analysis to highlight individuals that reported having more extreme concerns for either privacy or value. The resulting archetype distribution had 140 apathists, 55 protectionists, 69 capitalists, and 108 pragmatists. The following paragraphs detail the behavioral, cultural, and psychological findings in regard to these archetypes (see Table 2).

Behavioral Findings

Disclosure behavior was elicited by a scenario where respondents were randomly exposed to one of three privacy policies for a smartphone app that were identical except for the app domain context (i.e., travel, finance, and health) to test the impact of sensitivity of data disclosure. They were asked a single item (i.e., "Do you accept this privacy policy so you can use the app?" measured on a 5-point scale from "definitely no" to "definitely yes"). While the different app contexts did not show significant differences for disclosure decisions ($F(2,335) = 0.096$, $p = 0.908$), there were significant differences in the disclosure behavior between the archetypes ($F(3,335) = 17.49$, $p < 0.001$). Across all three app contexts, capitalists and apathists were significantly more likely to disclose information by accepting the terms and conditions stated in the privacy policy than pragmatists and protectionists.

The time that respondents used to read the app's privacy policy statement and make the decision to accept the policy and use the app was also recorded. While the different app contexts did not show significant differences for decision time

Table 2
Survey study results.

Variable descriptives			Attitude archetypes				One-way ANOVA	
Name	Mean	Std. Dev.	Apathists	Protectionists	Capitalists	Pragmatists	F(3,335)	*p* value
Decision time (seconds)	77.69	72.60	62.93^{a}	72.17	72.89^{b}	$97.77^{a,b}$	4.53	0.004
Decision to disclose	3.63	1.36	$4.14^{c,d}$	$3.09^{c,e}$	$4.06^{e,f}$	$3.12^{d,f}$	17.49	<0.001
Decision comfort	6.06	1.08	5.88^{h}	5.87^{g}	$6.41^{g,h}$	6.09	3.95	0.009
Uncertainty avoidance	4.22	0.62	$3.96^{i,j,m}$	$4.13^{j,l}$	$4.26^{k,m}$	$4.48^{i,k,l}$	14.60	<0.001
Collectivism	3.07	0.82	3.11	2.85	3.12	3.10	1.54	0.204
Long-term orientation	4.01	0.65	$3.57^{n,o,p}$	3.95^{n}	4.15^{o}	$4.38^{n,p}$	37.97	<0.001
Extraversion	3.51	1.55	3.31	3.51	3.52	3.69	1.07	0.362
Agreeableness	4.93	1.18	4.76^{q}	4.72^{r}	4.92	$5.20^{q,r}$	3.19	0.024
Conscientiousness	5.24	1.29	$4.78^{s,t}$	5.53^{s}	5.13^{u}	$5.62^{t,u}$	9.07	<0.001
Emotional stability	4.49	1.45	4.44	4.42	4.54	4.55	0.18	0.912
Open to new experiences	5.18	1.19	$.69^{v,x,y}$	5.22^{v}	5.42^{x}	5.47^{y}	9.60	<0.001
n	336		104	55	69	108		

Note: Superscripts indicate significant contrasting differences, $p < 0.05$.

(F(2,335) = 0.084, p = 0.919), there were significant differences between the archetypes in the time it took respondents to read the policy and make a decision (F(3,335) = 4.53, p = 0.004). Pragmatists took the longest time to read and decide to accept the policy compared to the other three archetypes, which were not significantly different from each other (F(2, 227) = 0.75, p = 0.472). This shows evidence that pragmatists, who have high privacy and high value concerns, spend significantly more time reading and considering their decision to accept the privacy policy than other respondents that have a dominant concern (i.e., capitalists and protectionists) or are relatively unconcerned with value and privacy (i.e., apathists). Thus, regardless of of the data sensitivity context these findings confirm that individuals have different decision processes depending on the salience of their personal concerns for value and privacy.

Furthermore, respondents were asked to report their comfort with their decision using a single-item (i.e., "How comfortable are you with your decision?" measured on a 7-point scale from "extremely uncomfortable" to "extremely comfortable"), which varied significantly across archetypes (F(3,335) = 3.95, p = 0.009). Capitalists were the most comfortable with their decisions to accept the privacy policy and use the app compared to pragmatists (t(175) = 1.99, p = 0.048), apathists (t(171) = 3.37, p = 0.001), and protectionists (t(122) = 2.746, p = 0.007). Pragmatists, protectionists, and apathists were similarly comfortable with their decision (F(2,264) = 1.45, p = 0.306). Thus, these results show that attitudes toward customer surveillance do impact disclosure decisions, decision time, and decision comfort.

Cultural Findings

Cultural contexts have been shown to have powerful impacts on behaviors, thus it is included here as potential influencing factors. Cultural dimensions were measured at the individual level using Yoo, Donthu, and Lenartowicz's (2011) scales for uncertainty avoidance (mean = 4.22, standard deviation = 0.62, alpha = 0.84), collectivism (mean = 3.07, standard deviation = 0.82, alpha = 0.82), and long-term orientation (mean = 4.01, standard deviation = 0.65, alpha = 0.75). Respondents reported significantly different levels of uncertainty avoidance among the four archetypes (F (3,335) = 14.60, p < 0.001) with pragmatists not tolerating uncertainty relatively well compared to apathists, while protectionists and capitalists were not significantly different from one another. Collectivism was similar among the archetypes (F(3,335) = 1.54, p = 0.204). Individuals' long-term orientation was significantly different between archetypes (F(3,335) = 37.97, p < 0.001) with pragmatists and capitalists caring more about the future compared to apathists or protectionists. Thus, these findings indicate that cultural dimensions are indeed associated with different attitudes toward customer surveillance.

Psychological Findings

Individuals' attitudes and behavior are shaped by their personality. Respondents' big five personality traits were measured using Gosling, Rentfrow, and Swann's (2003) scale: extraversion (mean = 3.51, standard deviation = 1.55), agreeableness (mean = 4.93, standard deviation = 1.18), conscientiousness (mean = 5.24, standard deviation =1.29), emotional stability (mean = 4.49, standard deviation = 1.45), and openness to new experiences (mean = 5.18, standard deviation = 1.19). There were no significant differences with regard to respondents' reported levels of extraversion (F(3,335) = 1.07, p = 0.362) or emotional stability (F(3,335) = 0.18, p = 0.912). The personality dimensions of agreeableness (F(3,335) = 3.19, p = 0.024), conscientiousness (F(3,335) = 9.07, p < 0.001), openness to new experiences (F(3,335) = 9.60, p < 0.001) were all significantly different across the attitude archetypes following similar patterns going from relatively low scores for apathists and protectionists to higher scores for capitalists and pragmatists. Thus, these results show that some of the big five personality dimensions (i.e., agreeableness, conscientiousness, and openness to new experiences) are associated with the archetypes of attitudes toward customer surveillance.

General Discussion

The results of two empirical studies first develop archetypes of attitudes toward customer surveillance, and then offer confirmatory evidence on the behavioral consequences and additional insight into potential antecedents of these attitudes. In the interview study, informants reported different reactions toward customer surveillance, and these reactions can be mapped onto the four attitude archetypes as illustrated above in Fig. 1. Table 3 reports a summary of these results across archetypes broken down into the three components of an attitude and serves as a useful comparison tool.

Despite variations in attitudes toward customer surveillance, many informants reported using a variety of obfuscation strategies. However, for the most part, these strategies were employed for very different reasons. Protectionist informants, for example, gave false or confusing data to firms to protect their personal privacy. Capitalist informants, in contrast, gave misleading data to prevent potential irritation from firms 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 and Culnan 2004), which found that participants either were concerned for their data privacy or simply wanted to avoid the irritation of junk email communication.

While protectionists and pragmatists expressed their consumer privacy concerns in both empirical studies, capitalists and apathists did not show much concern over consumer privacy. This finding supports many empirical studies (Dinev and Hart 2006; Malhotra, Kim, and Agarwal 2004; Milne and Bahl 2010; Phelps, Nowak, and Ferrell 2000) that claim that individuals have different responses to privacy and privacy threats.

As in privacy calculus research (Dinev and Hart 2006; Smith, Dinev, and Xu 2011; Xu et al. 2011), pragmatists in interviews reported having competing high consumer privacy concern and high consumer value concerns, suggesting a

Table 3
Comparison of attitudes toward customer surveillance.

	Personal concerns		Attitude components		
Attitude archetype	Consumer privacy	Consumer value	Thoughts	Feelings	Intended behaviors
Protectionists	High	Low	No trust; need for privacy protection	Feel threatened; surveillance = creepy	Predisposed to avoid customer surveillance
Capitalists	Low	High	Implicit contract with firms; trust firms	Enjoy utility and feelings of status	Predisposed to disclose data if the benefit is explicit
Pragmatists	High	High	Carefully consider the merits of each request	Want to enjoy benefits; worried about privacy	Calculate net benefits that include privacy costs
Apathists	Low	Low	Do not consider value or privacy important concerns	Bored and annoyed; feel a lack of control	Do not seek value but often provide data

rational decision process that results in longer decision times, which is confirmed in the survey study. For the other three archetypes, consumer privacy and consumer value concerns were found to be different or at low levels. Thus, decisions to disclose are less likely to be fully considered or calculated and might indicate the presence of decision heuristics, which may have been developed due to the dominant concern. Protectionists would not be satisfied with additional value in return for providing personal data, as their consumer privacy concerns likely cannot be diminished or subdued by increased offered value. Similarly, capitalists operate in the opposite fashion, where providing more consumer privacy assurance does not motivate increased disclosure of personal data, as they respond to value opportunities. Considering the S–O–R framework (Davis and Luthans 1980; Poddar, Mosteller, and Ellen 2009; Wang et al. 2019) again, individuals are responding to disclosure requests in ways to maximize their personal goals while minimizing cognitive effort. Thus, protectionists and capitalists are less likely to make calculated decisions and may rely instead on consumer privacy and value heuristics, respectively. Regardless of either consumer value offered or consumer privacy threats, apathists report a lack of concern for both value and privacy, and thus are likely to be influenced by external factors. Alternatively, these responses could be explained using the theory of learned helplessness (Maier and Seligman 1976, 2016), as apathists may believe they cannot effectively manage their data privacy. Using these four attitude archetypes, marketing researchers and managers can understand how individuals are predisposed to customer surveillance and develop strategies to both protect relationships while gaining valuable consumer data.

Managerial Implications

Attitudes toward customer surveillance are important for firms to consider when making decisions regarding customer surveillance activities, privacy policies, segment targeting, or customer surveillance disaster response. In the interview study, most informants advised firms to be more transparent and explicit about consumer privacy risks and potential consumer value derived from disclosing personal data.

As protectionist consumers are chiefly concerned with limiting their consumer privacy risks, offering more information about how their personal data would be collected, stored, and used, as well as offering assurances of data security, might allay some of these concerns. However, this additional information also highlights the firm's customer surveillance activities and perhaps a more strategic approach is needed. Firms might target protectionist consumers by offering specific, customized services to ensure that their personal data concerns 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. By designing these privacy-aware products and services, firms can strategically create much value in the minds of protectionist consumers that are predisposed to reduce privacy risks.

Capitalist consumers care primarily about deriving the most consumer value out of their data resources. Firms can strategically target capitalists by highlighting the explicit benefits available to those disclosing data, including for example added convenience, enhanced services, exclusive information, or additional discounts. Using a credit card example again, capitalists might prefer an offer that includes location-specific personalized services and discounts for disclosing real-time location data to the credit card company. Firms can reimagine products and services by explicitly using capitalist consumers' data to enhance the utilitarian and hedonic benefits available to these consumers that are predisposed to seek out value.

While apathists may not worry about either consumer privacy or consumer value, these consumers do likely worry about other firm attributes. These attributes can be discovered through market research and may include, for example, enhanced corporate social responsibility programs, leading corporate ethics policies, brand status, or brand reputation.

Managers can develop strategic customer surveillance activities that are sensitive to these archetypes by personalizing the level of personal information disclosure requested, thus protecting customer relationships while providing valuable customer data. In doing so, managers may successfully attract new “blue sky” segments that are not having their specific needs serviced by any provider through strategies that offer enhanced privacy protection services, more explicit value opportunities, or clearer information about the privacy risks and benefits.

Toward a Research Agenda

Customer surveillance is an important part of marketing that ensures that firms have the data they need to innovate their products and services to remain competitive. While this article introduces and explores attitudes toward customer surveillance, there are several avenues that researchers could investigate in the future. A research agenda is outlined below to develop a robust understanding of how these attitudes impact consumers and their decisions.

The *disclosure context* and its associated variables likely also contribute to consumer reactions to customer surveillance. Although the data sensitivity context was not significant in the survey study, contextual variables are likely to be factors contributing to consumer responses to data disclosure requests, such as for example firm relationship strength, customer satisfaction, firm positioning, firm attributed status, firm reputation, or severity of privacy threat. Future research should consider how variations in the attitude toward customer surveillance may or may not influence the perception or salience of the context surrounding a data disclosure request.

The *tenuous connection* between attitudes toward customer surveillance and attitudes toward general or government surveillance needs to be investigated. This is to understand, compare, and contrast how attitudes formed in the consumer environment are different from those in other environments. Further research could explore other social, demographic, cultural, and psychographic variables that may impact the relationship between consumer surveillance, general surveillance, and other specific types of surveillance.

The *stability* of these attitudes needs to be uncovered. Future research could examine how individuals' attitudes change over time, as it is unclear how age or extraordinary experiences change individuals' attitude toward customer surveillance. Moreover, research can explore how consumers react to significant or prolonged experiences with customer surveillance.

The *cognitive decision process* when facing disclosure requests needs to be further assessed, as it appears that these attitudes can both rationally and heuristically influence these decisions. The findings of both studies provide a boundary to the utility of the privacy calculus concept, namely, individuals that do not have high consumer privacy and high consumer value concerns likely use a mix of rational and heuristic processing to arrive at their disclosure decisions. More research is needed into heuristic decisions to disclose or not disclose personal data, and also how these heuristic decision rules are formed. Furthermore, research needs to uncover under what conditions cue the rational process that supersedes dominant concern-based heuristics. Additional research could further investigate the extent to which data disclosure decisions are made using heuristic-based or analysis-based processes using experimental or brain imaging methods.

Value concerns have been researched extensively but within a narrow, price promotions context. However, consumer value is much broader than this context and this article provides more insight into how value concern changes consumer decisions when faced with personal data disclosure requests. Future research could examine the motivational aspects of hedonic and utilitarian benefits on the decision to disclose personal data. These findings could be applied to consumer engagement, marketing communications, firm positioning, and other marketing strategies.

Privacy concerns have been well researched in the literature, but little emphasis has been placed on how consumers perceive customer surveillance. In the age of big data, different customer surveillance methods of collecting, storing, and using market intelligence might increase or allay consumer privacy concerns. Further research is needed to understand how consumer privacy concerns can be mitigated to better design products, services, and corporate privacy policies that are customized to attractive consumer segments.

Although the informant sample provided valuable depth on these attitudes, *additional factors* not explored in this research that impact attitudes toward customer surveillance could be identified using other conceptual lenses or other research methods.

This article introduces and conceptualizes attitudes toward customer surveillance that can account for responses to these types of surveillance. It explores these attitudes further through a series of consumer interviews resulting in four attitude archetypes. Then, using survey evidence, it confirms the behavioral consequences of these archetypes and shows how they are associated with cultural and psychological factors. Based on these archetypes, the article suggests how managers can protect customer relationships by using these attitudes to alter their product, services, privacy policies, customer surveillance practices. The article closes by presenting a research agenda that offers several avenues for researchers to further investigate how customer surveillance practices impact consumer behavior.

Acknowledgements

This research was partly funded by The Social Sciences and Humanities Research Council of Canada (SSHRC) Doctoral Grant Program and the British Academy/Leverhulme Trust Small Grant Scheme (SG152776) both awarded to the first author. The Authors would like to acknowledge the editorial guidance of Dr. Ratchford, the useful comments of the two anonymous reviewers, and the feedback on previous drafts of Dr. Leyland Pitt, Dr. Rick Watson, and Dr. Michael Parent.

References

Ailawadi, Kusum L., Scott A. Neslin, and Karen Gedenk (2001), "Pursuing the Value-Conscious Consumer: Store Brands Versus National Brand Promotions," *Journal of Marketing*, 65, 1, 71–89.

Ajzen, Icek (2011), "The Theory of Planned Behaviour: Reactions and Reflections," *Psychology & Health*, 26, 9, 1113–27.

——— and Martin Fishbein (1977), "Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research," *Psychological Bulletin*, 84, 5, 888–918.

Albrechtslund, Anders (2008), "Online Social Networking as Participatory Surveillance," *First Monday*, 13, 3.

Alford, Bruce L. and Abhijit Biswas (2002), "The Effects of Discount Level, Price Consciousness and Sale Proneness on Consumers' Price Perception and Behavioral Intention," *Journal of Business Research*, 55, 9, 775–83.

Andrejevic, Mark (2007), *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: University of Kansas Press.

Arnold, Stephen J. and Eileen Fischer (1994), "Hermeneutics and Consumer Research," *Journal of Consumer Research*, 21, 1, 55–70.

Babin, Barry J., William R. Darden, and Mitch Griffin (1994), "Work and/or Fun: Measuring Hedonic and Utilitarian Shopping Value," *Journal of Consumer Research*, 20, 4, 644–56.

Bargh, John A., Peter M. Gollwitzer, Annette Lee-Chai, Kimberly Barndollar, and Roman Trotschel (2001), "The Automatic Will: Nonconscious Activation and the Pursuit of Behavioral Goals," *Journal of Personality and Social Psychology*, 81, 6, 1–40.

Bauman, Zygmunt and David Lyon (2013), *Liquid Surveillance: A Conversation*. Cambridge, UK: Polity Press.

Baumgartner, Hans (2002), "Toward a Personology of the Consumer," *Journal of Consumer Research*, 29, 2, 286–92.

Berry, Michael J. and Gordon S. Linoff (2004), *Data Mining Techniques: for Marketing, Sales, and Customer Relationship Management*. Indianapolis, IN: Wiley Publishing.

Blattberg, Robert C. and John Deighton (1991), "Interactive Marketing: Exploiting the Age of Addressability," *Sloan Management Review*, 33, 1, 5–15.

Bucklin, Randolph E. and Catarina Sismeiro (2003), "A Model of Web Site Browsing Behavior Estimated on Clickstream Data," *Journal of Marketing Research*, 40, 3, 249–67.

——— and ——— (2009), "Click Here for Internet Insight: Advances in Clickstream Data Analysis in Marketing," *Journal of Interactive Marketing*, 23, 1, 35–48.

Creswell, John W. (2009), *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Los Angeles, CA: Sage.

Culnan, Mary J. and Pamela K. Armstrong (1999), "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, 10, 1, 104–15.

Davis, Tim R. and Fred Luthans (1980), "A Social Learning Approach to Organizational Behavior," *Academy of Management Review*, 5, 2, 281–90.

Deighton, John and Leora Kornfeld (2009), "Interactivity's Unanticipated Consequences for Marketers and Marketing," *Journal of Interactive Marketing*, 23, 1, 4–10.

Dinev, Tamara and Paul Hart (2006), "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, 17, 1, 61–80.

———, Allen R. McConnell, and H. Jeff Smith (2015), "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research*, 26, 4, 639–55.

Fournier, Susan (1998), "Consumers and Their Brands: Developing Relationship Theory in Consumer Research," *Journal of Consumer Research*, 24, 4, 343–53.

Gosling, Samuel D., Peter J. Rentfrow, and William B. Swann (2003), "A Very Brief Measure of the Big-Five Personality Domains," *Journal of Research in Personality*, 37, 6, 504–28.

Hill, Ronald P. and Mark Stamey (1990), "The Homeless in America: An Examination of Possessions and Consumption Behaviors," *Journal of Consumer Research*, 17, 3, 303–21.

Holtrop, Niels, Jaap E. Wieringa, Maarten J. Gijsenberg, and Peter C. Verhoef (2017), "No Future Without the Past? Predicting Churn in the Face of Customer Privacy," *International Journal of Research in Marketing*, 34, 1, 154–72.

Jaworski, Bernard J. and Ajay K. Kohli (1993), "Market Orientation: Antecedents and Consequences," *Journal of Marketing*, 57, 3, 53–70.

John, Leslie K., Alessandro Acquisti, and George Loewenstein (2011), "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research*, 37, 5, 858–73.

Junglas, Iris A. and Rick T. Watson (2008), "Location-Based Services," *Communications of the ACM*, 51, 3, 65–9.

Kahneman, Daniel (2011), *Thinking Fast and Slow*. Toronto, ON: Doubleday Canada.

Kim, Hyejeong and Linda S. Niehm (2009), "The Impact of Website Quality on Information Quality, Value, and Loyalty Intentions in Apparel Retailing," *Journal of Interactive Marketing*, 23, 3, 221–33.

Kohli, Ajay K. and Bernard J. Jaworski (1990), "Market Orientation: The Construct, Research Propositions, and Managerial Implications," *Journal of Marketing*, 54, 2, 1–18.

Krafft, Manfred, Christine M. Arden, and Peter C. Verhoef (2017), "Permission Marketing and Privacy Concerns—Why Do Customers (Not) Grant Permissions?" *Journal of Interactive Marketing*, 39, 1, 39–54.

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

Lee, Leonard and Dan Ariely (2006), "Shopping Goals, Goal Concreteness, and Conditional Promotions," *Journal of Consumer Research*, 33, 1, 60–70.

Lichtenstein, Donald R., Richard G. Netemeyer, and Scot Burton (1990), "Distinguishing Coupon Proneness from Value Consciousness: An Acquisition-Transaction Utility Theory Perspective," *Journal of Marketing*, 54, 3, 54–67.

Lyon, David (2007), *Surveillance Studies: An overview*. Cambridge, UK: Polity Press.

Maier, Steven F. and Martin E. Seligman (1976), "Learned Helplessness: Theory and Evidence," *Journal of Experimental Psychology: General*, 105, 1, 3.

——— and Martin E.P. Seligman (2016), "Learned Helplessness at Fifty: Insights from Neuroscience," *Psychological Review*, 123, 4, 349.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, 15, 4, 336–55.

Marchand, André and Thorsten Hennig-Thurau (2013), "Value Creation in the Video Game Industry: Industry Economics, Consumer Benefits, and Research Opportunities," *Journal of Interactive Marketing*, 27, 3, 141–57.

Marshall, Nancy J. (1972), "Privacy and Environment," *Human Ecology*, 1, 2, 93–110.

McCombs, Maxwell (2004), *Setting the Agenda: The Mass Media and Public Opinion*. Cambridge, UK: Polity Press.

Mehta, Raj and Russel W. Belk (1991), "Artifacts, Identity, and Transition: Favorite Possessions of Indians and Indian Immigrants to the United States," *Journal of Consumer Research*, 17, 4, 398–411.

Milne, George R. and Shalini Bahl (2010), "Are There Differences Between Consumers' and Marketers' Privacy Expectations? A Segment-and Technology-Level Analysis," *Journal of Public Policy & Marketing*, 29, 1, 138–49.

——— and Mary J. Culnan (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.

Moe, Wendy W. and Brian T. Ratchford (2018), "How the Explosion of Customer Data has Redefined Interactive Marketing," *Journal of Interactive Marketing*, 42, 1, A1–2.

Morgan, Robert M. and Shelby D. Hunt (1994), "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing*, 58, 3, 20–38.

Mosteller, Jill and Amit Poddar (2017), "To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors," *Journal of Interactive Marketing*, 39, 1, 27–38.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell (2000), "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing*, 19, 1, 27–41.

Plangger, Kirk and Rick T. Watson (2015), "Balancing Customer Privacy, Secrets, and Surveillance: Insights and Management," *Business Horizons*, 58, 6, 625–33.

Poddar, Amit, Jill Mosteller, and Pam Scholder Ellen (2009), "Consumers' Rules of Engagement in Online Information Exchanges," *Journal of Consumer Affairs*, 43, 3, 419–48.

Shankar, Venkatesh, Mirella Kleijnen, Suresh Ramanathan, Ross Rizley, Steve Holland, and Shawn Morrissey (2016), "Mobile Shopper Marking: Key Issues, Current Insights, and Future Research Avenues," *Journal of Interactive Marketing*, 34, 37–48.

Sherry Jr., John F. (1990), "A Sociocultural Analysis of a Midwestern American Flea Market," *Journal of Consumer Research*, 17, 1, 13–30.

Sheth, Jagdish N., Bruce I. Newman, and Barbara L. Gross (1991), "Why We Buy What We Buy: A Theory of Consumption Values," *Journal of Business Research*, 22, 2, 159–70.

Shmargad, Yotam and Jameson K. Watts (2016), "When Online Visibility Deters Social Interaction: The Case of Digital Gifts," *Journal of Interactive Marketing*, 36, 1, 1–14.

Smith, H. Jeff, Tamara Dinev, and Heng Xu (2011), "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, 35, 4, 989–1016.

———, Sandra J. Milberg, and Sandra J. Burke (1996), "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly*, 20, 2, 167–96.

Turow, Joseph (2008), *Niche Envy: Marketing Discrimination in the Digital Age*. Cambridge, MA: MIT Press.

Wang, Wei, Renee Rui Chen, Carol X. Ou, and Steven J. Ren (2019), "Media or Message, Which Is the King in Social Commerce?: An Empirical Study of Participants' Intention to Repost Marketing Messages on Social Media," *Computers in Human Behavior*, 93, 176–91.

Wood, David M. and Kirstie Ball (2013), "Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neo-Liberal Capitalism," *Marketing Theory*, 13, 1, 47–67.

Woodruff, Robert B. (1997), "Customer Value: The Next Source for Competitive Advantage," *Journal of the Academy of Marketing Science*, 25, 2, 139–53.

Xu, Heng, Dinev Tamara, H. Jeff Smith, and Paul Hart (2011), "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems*, 12, 12, 798–824.

Yoo, Boonghee, Naveen Donthu, and Tomasz Lenartowicz (2011), "Measuring Hofstede's Five Dimensions of Cultural Values at the Individual Level: Development and Validation of CVSCALE," *Journal of International Consumer Marketing*, 23, 3–4, 193–210.

Yoon, Sukki and Patrick T. Vargas (2010), "Feeling Happier when Paying More: Dysfunctional Counterfactual Thinking in Consumer Affect," *Psychology & Marketing*, 27, 12, 1075–100.

Zeithaml, Valarie A. (1988), "Consumer Perceptions of Price, Quality, and Value: A Means-End Model and Synthesis of Evidence," *Journal of Marketing*, 52, 3, 2–22.