Journal of the Association for Information Systems

Volume 18 | Issue 11 Article 3

11-30-2017

Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption?

Merrill Warkentin
Mississippi State University, m.warkentin@msstate.edu

Sanjay Goel
University at Albany, SUNY, goel@albany.edu

Philip Menard
University of South Alabama, pmenard@southalabama.edu

Recommended Citation
Warkentin, Merrill; Goel, Sanjay; and Menard, Philip (2017) "Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption?," *Journal of the Association for Information Systems*, 18(11), .
DOI: 10.17705/1jais.00474
Available at: https://aisel.aisnet.org/jais/vol18/iss11/3

Journal of the Association for Information Systems

Research Paper ISSN: 1536-9323

Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption?

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Sanjay Goel
State University of New York at Albany
goel@albany.edu

Philip Menard
University of South Alabama
pmenard@southalabama.edu

Abstract:

An unexplored gap in IT adoption research concerns the positive role of shared benefits even when personal information is exposed. To explore the evaluation paradigm of shared benefits versus the forfeiture of personal information, we analyze how utility consumers use smart metering technology (SMT). In this context, utility companies can monitor electricity usage and directly control consumers' appliances to disable them during peak load conditions. Such information could reveal consumers' habits and lifestyles and, thus, stimulating concerns about their privacy and the loss of control over their appliances. Responding to calls for theory contextualization, we assess the efficacy of applying extant adoption theories in this emergent context while adding the perspective of the psychological ownership of information. We use the factorial survey method to assess consumers' intentions to adopt SMT in the presence of specific conditions that could reduce the degree of their privacy or their control over their appliances and electricity usage data. Our findings suggest that, although the shared benefit of avoiding disruptions in electricity supply (brownouts) is a significant factor in electricity consumers' decisions to adopt SMT, concerns about control and information privacy are also factors. Our findings extend the previous adoption research by exploring the role of shared benefits and could provide utility companies with insights into the best ways to present SMT to alleviate consumers' concerns and maximize its adoption.

Keywords: IS Security, Privacy, Smart Metering, Smart Grid, Privacy, Monitoring, Factorial Survey Method, Technology Acceptance, Psychological Ownership, Trust, Shared Benefits.

Suprateek Sarker was the accepting senior editor. This paper was submitted November 25, 2013, and went through 4 revisions.

1 Introduction

The extant research on individual decisions to adopt information technologies has addressed a plethora of variables that influence the decision process. In addition to effort expectancy, performance expectancy, and social influence, research has investigated many other beliefs and perceptions related to adoption in various contexts and individuals' rational assessments of perceived associated costs and benefits. However, the information systems (IS) research community has not yet empirically evaluated the role of *shared benefits*. Such benefits accrue to the entire society and are factors in individuals' decisions to adopt a technology. To fill this gap in the IS literature, we extend the existing theoretical frameworks of information privacy and technology adoption by examining the role of shared benefits in decisions to adopt smart metering technology (SMT).

In this study, we also evaluate the role of *the perceived psychological ownership of information* in influencing users' perceptions of privacy, which we identify as a salient factor in technology adoption decisions. To investigate this nomological network, we chose SMT, which research has not yet fully scrutinized but provides an ideal opportunity to explore the unique relationships often found in these contexts. For instance, in the case of individual consumers' adopting smart meters, consumers may realize *shared benefits* due to the collective utility savings of avoiding the need for expensive peak demand power generation, decreased dependence on fossil fuels, reduced greenhouse emissions, and increased national energy security. These shared factors may overshadow the allure of the *direct benefit*: personal financial savings gained from adopting smart meters.

1.1 Theory Contextualization

Management scholars have called for improving theory formation (Gregor & Klein, 2014) and theory contextualization to increase the rigor of the theorizing process and the theories themselves. Johns (2006) shows how context could influence theory and theorizing. Salovaara and Merikivi (2015) suggest that, by re-examining published studies to verify or extend their findings, researchers could increase the knowledge of the *boundary conditions* of existing theories and strengthen the research community by accelerating the exchange of information between researchers. Seddon and Scheepers (2012, 2015) reiterate this recommendation and suggest that the boundary conditions of published studies be tested to determine whether the original findings could be replicated in a new environment or not. Joshi and Roh (2009) provide a roadmap for context-focused research and urge researchers to account for context more carefully in their research, which would facilitate greater theoretical integration of both macro- and micro-levels of analysis and pave the way for new theoretical developments. Researchers have described context in various ways. For instance, Cappelli and Sherer (1991) define it as the surroundings that help illuminate the focal phenomenon. Johns (2006) defines context as the surrounding phenomena that are external to the focus of the study, such as the individual, which often exist at a different level of analysis. Whetten (2009) provides a framework for cross-context theorizing and explicates how theory contextualization determines the extent to which a theory explicitly accounts for relevant contextual conditions and enables scholars to provide a theoretical contribution.

In an editorial in the *Academy of Management Journal*, Bamberger (2008) suggests that, in our research, we can and should increasingly give greater consideration to the role of context—"that amorphous concept capturing theory-relevant, surrounding phenomena or temporal conditions" (p. 839). He recommends that authors should "incorporate into their theoretical models how particular situational or temporal factors…might play a role in explaining the phenomena they are examining" (p. 844). He also suggests that scholars should actively challenge the boundary assumptions of the paradigms in which their theories are nested in a process that he terms context theorizing to specify how surrounding phenomena influence the theories' variables.

Sarker (2016) argues for a balance between theoretical abstractions that provide *contextual specificity* and *generality*. He concurs that we need to contextualize our findings by identifying relevant boundary conditions, but he also respects the generalizability of good theory albeit without subscribing to *universalism.* Recognizing Johns' (2006) differentiation between broad features in the omnibus category of context (e.g., who, where, what, and why) and the discrete category, Sarker suggests that we should "deliberately select" our level of abstraction and the contextual elements to include so that our contribution can be clearly associated with explicit boundary conditions. We follow Sarker's recommendation to identify the omnibus contextual elements before specifying the discrete context of our study.

Finally, Hong, Chan, Thong, Chasalow, and Dhillon (2014) argue for the importance of context in theory development and identify meaningful ways that IS research studies have been and could be extended to new contexts in order to establish construct validity in cross-context research. In this way, theories would be strengthened and improved (Whetten, Felin, & King, 2009). Kahneman (2012) suggests that scientists overly trust their findings and do not verify them sufficiently. Lee and Baskerville (2003, 2012) imply that IS researchers are similarly guilty and suffer from angst with regard to the right "sweet spot" for concluding the generalizability of findings. Olbrich, Frank, Gregor, Niederman, and Rowe (2016, p. 2) point out that IS authors "should be as sensitive to context as they are attentive about making modifications to instruments and theories to suit the context of their study", yet they also recognize that such sensitivity may limit their ability to verify previous studies. Against this backdrop, we apply and contextualize adoption theories in the important and unique context of SMT adoption and shared benefits in order to strengthen and contribute to our theoretical understanding of the nomological network.

1.2 Smart Metering Technology

Although energy consumption throughout the world has trended upward for many years, it may not be sustainable. Many electricity consumers in the US, Europe, and elsewhere have concerns about personally reducing their consumption to reduce costs to themselves. They often also influence national energy policy regarding sustainability and environmental impact (Brooks, Wang, & Sarker, 2012; Califf, Lin, & Sarker, 2012; Wang, Brooks, & Sarker, 2015a, 2015b; Watson, Boudreau, & Chen, 2010). But consumers also have legitimate concerns about maintaining the security and privacy of their personal information (Goel, Williams, & Dincelli, 2016; James, Nottingham, Collignon, Warkentin, & Ziegelmayer, 2016; Lee, Crossler, Otondo, & Warkentin, Forthcoming), and, because these concerns are key to their adopting the smart electric grid (i.e., smart grid), they have rekindled the debate on the fundamental premise of anonymity on the Internet (Goel, 2015). The electric grid runs to capacity in some areas, which makes it prone to large-scale failures (also known as blackouts), such as those recently witnessed in widespread disruptions of power in Europe and North America. In other cases, when the peak demand for electricity exceeds the current supply, electricity is rationed through controlled (intentional) power disruption (voltage reduction or limited-area blackouts) across different neighborhoods in a phenomenon commonly known as brownouts. The concept of the smart grid emerged in the aftermath of these blackouts to increase the system's resilience through implementing information technologies. The smart grid superposes a communication network over the existing electrical grid, which enables managers to collect information about electrical power production, transmission, and consumption in order to monitor its operational state and, thereby, improve its efficiency and stability. The communication network, coupled with sensors deployed across the grid, provides information about the grid's state, which allows one to isolate faults and operations to resume across the unaffected parts of the grid. This new technology, which electricity producers and distribution utilities are phasing in, is designed to gradually increase the efficiency of production and distribution by actively reducing peak demand and the likelihood of blackout conditions without the need to construct additional expensive peak-load demand plants (Potter, Archambault, & Westrick, 2009; Wunderlich, Veit, & Sarker, 2012a).

1.2.1 Smart Meters

The communication network on the smart grid ideally should extend to the *last mile* in connecting each consumer to the local utility network. The smart grid vision incorporates SMT at the consumer's location (both household and business consumers) either as an increased-functionality external meter or as a smart system tied to specific appliances and electric components in their premises (Darby, 2010; Wunderlich, Veit, & Sarker, 2012b). These smart meters would allow two-way metering of power and to provide detailed information about usage to both utility companies and consumers. Smart meters in individual households would enable consumers to actively manage the electricity they consume, which would allow them to stop using non-essential appliances during peak demand and shift to reduced-cost periods, such as nighttime hours, if they are available as a service provided by their local utility company (Fridgen, Häfner, König, & Sachs, 2016). Smart meters would also allow consumers to monitor and evaluate appliance usage patterns for potential reductions in electricity consumption. The highly detailed monitoring that SMT employ could result in better service for consumers, reduce operating costs for power companies, and mitigate environmental concerns associated with energy consumption (Wunderlich et al., 2012b). Smart grid technologies could also enable electricity utilities to actively disable non-essential appliances in selected households, which would preclude the need to build and use costly peak-load demand plants. Although most locations do not yet have SMT, consumers meet them when deployed with varying degrees of resistance—even if they bring financial benefits (Kostyk & Herkert, 2012).

1.2.2 Customer Interaction

Rolling out SMT in a utility grid represents a notable change in how an electric company interacts with its customers. For a prominent shift in institutional or infrastructural policies to be successful, the affected consumers must possess sufficient goodwill toward the institution that initiates the change. These consumers must also be willing to perform collective actions as a unified community, which is especially pertinent in situations that involve policy changes related to global climate concerns (Adger, 2003). Although a regional utility company's rollout of smart meters may not directly relate to climate change, the reduction of energy consumption constitutes a key tenet of green initiatives (Lei & Ngai, 2013) and has been recently identified as an important area of research that needs more exploration in IS (Gholami, Watson, Hasan, Molla, & Bjørn-Andersen, 2016). The collective action (i.e., adopting energy conservation techniques) required for the success of such initiatives must include a societal element that influences the public, which does not exist in other adoption contexts. Furthermore, a unique aspect of technology adoption in the SMT context is that, in addition to altruistic societal benefits, selfish benefits affect both the individual and the community. An individual can only benefit from adopting SMT (avoiding rolling blackouts in particular) if the individual's community also adopts it.

We contribute to the theoretical understanding of this important phenomenon by addressing the roles of the shared benefit and psychological ownership in individual decisions to adopt SMT. In addition to the resistance to adoption attributable to the perceived of loss of control of privacy and data, consumers may also be concerned about others' using or misusing' the data that SMT captures about their electricity consumption patterns, including usage timing, type of use (categorized by appliance, room, or individuals in the household, etc.), and other data or metadata generated that the technology generates (Goel, Bush, & Neuman, 2013; Hess & Coley, 2012; Kostyk & Herkert, 2012; Systems, McDaniel, & McLaughlin, 2009). The technology collects and relays information about the energy use of each appliance in households to the utility company in short intervals (~15min). Each appliance (e.g., refrigerator, washing machine, etc.) has a unique load signature that the technology can separate from the overall load signature of a household and, thus, reveal intimate details of the household's activities, such as whether the occupants are cooking, washing clothes, watching television, or working on a computer. McKenna, Richardson, and Thompson (2012) identify several concerns that consumers have about how various parties could (mis)use their data; for example, burglars could use it to determine when houses are unoccupied, marketers could use it for profiling, law-enforcement agencies could use it to detect illegal activities, landlords could use it to dispute occupancy, and individuals could use it to spy on their family members, co-inhabitants, or community members. Although consumers may care primarily about data breaches at the individual level, power companies may also become potential targets for attackers who seek to obtain data from a large number of consumers (similar to hacks perpetrated on credit card companies or large retailers). Individuals may assume that they have the right to privacy in their homes, and they may view monitoring (i.e., data collection) by smart metering as violating that privacy (Gupta, 2012). Privacy concerns also extend to consumers' fearing the government will intrude into their personal lives and misuse their data for legal purposes.

1.2.3 Additional Advantages

Although smart meter technologies do not provide significant value to consumers in terms of their traditional function of metering compared to traditional electricity meters, they create considerable downstream advantages. First, consumers with smart meters can better realize their specific electricity usage and can manage their electricity usage to minimize expenses. Second, they can enjoy advanced services through their smart meters, such as appliance diagnostics and repairs, demand load management, and the ability to profit from selling unused renewable energy generation back to the grid. Consumers' desire to protect the environment by supporting an infrastructure that allows the grid to incorporate renewable energy sources may also strengthen their desire to adopt SMT.

Nevertheless, whether or not consumers adopt this technology presents a complex problem rooted in their behavior. To address this issue, Xu, Venkatesh, Tam, and Hong (2010) present a model that explains how and why consumers migrate to or adopt the new generation of an IS platform. They suggest that three things primarily drive IS technology migration: technology perceptions, external influences, and technology complementarities. The authors suggest that the level of change in technology (i.e., incremental, leapfrogging, or transformative) moderates the decision. Further, they suggest that users' perceptions of usefulness, ease of use, and monetary value most influence whether they adopt transformative technologies.

Smart meters constitute a transformative technology shift. Consequently, usefulness, ease of use, and monetary value are clearly key variables in users' perception of smart meters. Accordingly, presenting users with the comprehensive short- and long-term benefits of the technology would be an important influence in addition to the extrinsic incentives. Ease of use is also important because the different interfaces used with the technology affect it. Xu et al. (2010) do not consider the perceptions of security and privacy, which have become very important for consumers in the wake of the media's attention to recent breaches. Additionally, utilities must provide sufficient compensation to their customers for the privilege to control energy consumption at the individual-device level (Fridgen et al., 2016). This study fills this specific gap in the research by examining how consumers view the adoption of smart meters according to their perceptions of security and privacy.

In this section, we describe the study's context. Following Sarker's (2016) guidelines, we identify the omnibus category contextual factors by articulating the boundary conditions (who, where, when, and why) that may limit the generalizability of our findings. Specifically, we address the perceptions of the electric utility customers (homeowners) who are considering adopting smart meters (*who*) prior to a smart meter rollout (*when*) in the US (*where*) with information privacy concerns being a potential adoption barrier (*why*). Given this context, we proceed to identify the applicable theoretical foundations for our investigation. With our research method, we explore the discrete contextual elements that relate to the specific technological capabilities of SMT that we articulate above.

1.3 Technology Adoption in the Privacy Context

We need to understand the issues of privacy and control that arise from implementing SMT, to identify the drivers that dissuade consumers from adopting it, and to prevent them from changing their behavior either through self-management or through the demand-response that utility companies control. We need to address these concerns to increase consumers' acceptance and adoption of technology (Huang & Palvia, 2016). We need to educate consumers about SMT and we must use technology solutions to solve the challenges associated with anonymizing data as it moves from households to utilities.

Although researchers have previously explored the relationship between information privacy concerns and technology adoption, they have not sufficiently examined the role of privacy concerns in the context of SMT adoption, especially with regard to shared benefits. Privacy issues in SMT are unique because the forfeiture of certain information related to electricity consumption could directly lead to the shared benefit for a neighborhood or community; namely, avoiding brownouts. The U.S. homeowners we surveyed for this study indicated that this shared benefit was the only significant factor that could persuade them to adopt SMT despite potential privacy concerns. Studying the SMT context with specific regard to privacy may also reveal some unique characteristics of individuals' perceptions about personal privacy and of the potential benefits of sharing information for the greater good of communities. These shared benefits also inform our understanding of technology adoption.

In this study, we address the following research questions:

RQ1: What is the influence of perceived shared benefits on individual decisions, in which the outcomes may convey shared benefits in addition to or instead of individual benefits?

RQ2: How do consumers' concerns about information privacy influence their intentions to adopt smart metering technology?

RQ3: Which perceived benefits of adopting smart metering technology alleviate consumers' concerns associated with information privacy?

RQ4: Does psychological ownership of electricity usage information affect consumers' information privacy concerns?

Our findings about this context of smart metering technology contribute to explaining the range of decisions individuals make to adopt technologies that result in shared benefits rather than (or in addition to) individual benefits.

2 Hypothesis Development

The theoretical foundations of the research on SMT adoption rest in technology adoption models that researchers have extensively applied to a broad range of contexts of technology adoption. We developed our model from the several precedent models that we describe in considerable depth in this section. Following Hong et al.'s (2014) theory-contextualization guidelines, we leveraged elements of the well-established technology adoption theories and contextualized them by incorporating appropriate constructs relevant to the homeowner's perspective when assessing potential SMT use. We augmented the core theory construct of social influence with the psychological ownership construct that is relevant to the privacy concern context of the target environment. We incorporated the trust-risk framework and privacy concerns, which are central to formulating individuals' intentions and behaviors regarding information privacy, into our research model as well. Similar to Breward, Hassanein, and Head (Forthcoming), we formulated context-sensitive versions of the core theory constructs to create an approach that allowed the contextual variables to directly influence the underlying theory (Bagozzi, 2007; Whetten, 2009). Our research model includes existing factors (in Figure 1, the left side of the model) that represent subjective perceptions and beliefs and the manipulated factors (in Figure 1, see the right side of the model) of program discount, third party access, and meter invasiveness, which varied in the experimental design.

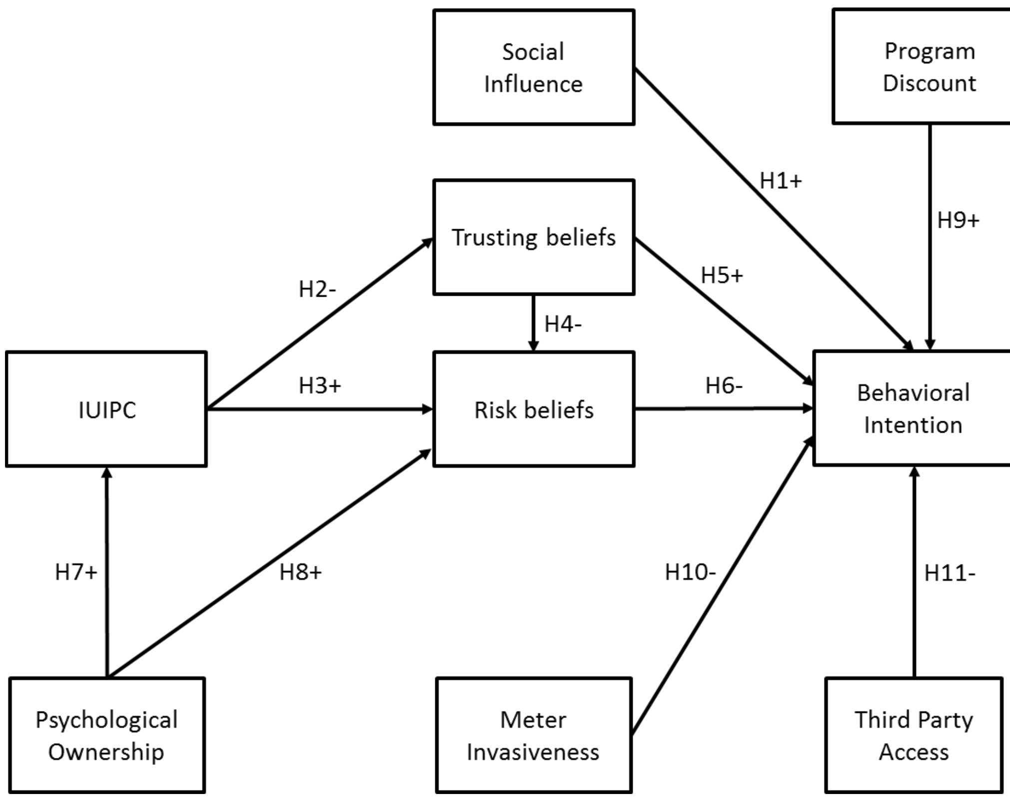

Figure 1. Conceptual Model

2.1 Technology Adoption

Because we examine the factors that influence consumers' acceptance of smart metering technology, we need to consider variables included in the UTAUT model (Venkatesh, Morris, Davis, Davis, & Hall, 2003). Despite the explanatory power of these constructs, many of them do not apply to the SMT-adoption context. Compared to other forms of technology, most consumers who have adopted SMT interact minimally with their smart meters and typically use them for nothing more than monitoring, although certain high-adoption areas (e.g., Ontario in Canada, Denmark, etc.) have witnessed the expanded use of the new data through home-energy management systems (HEMS). In this study, we focus on consumers' decision to adopt SMT or not. Utility companies install smart meters, which alleviates consumers' apprehensions concerning their competency to install or operate such a device. Furthermore, the utility company selects the hardware required for smart meter installation, so consumers are not involved in decisions about specific features and functions. For these reasons, we exclude performance expectancy, effort expectancy, and facilitating conditions, which the UTAUT includes, from the research model we use here.

Conversely, social influence could be applicable in the SMT context. In situations that involve potentially adopting an emerging technology, consumers often rely on word of mouth to inform their decisions about whether to do so (Cheung, Lee, & Rabjohn, 2008; Fichman, 2000; Gatignon & Robertson, 1989; Geroski, 2000; Li, 2004). Some examples include wireless Internet (Lu, Yu, Liu, & Yao, 2003), m-commerce (Okazaki, 2005), and social network sites (Chu, 2009). Similarly, energy consumers would likely rely on the opinions of important friends or colleagues to evaluate the possibility of adopting an emerging technology such as the smart meter. Considering the potential concerns and ramifications of sharing private usage information, the endorsement of important others could assist utility companies in persuading apprehensive customers to adopt SMT. Thus, we hypothesize:

> **H1:** Social influence positively influences behavioral intention to adopt smart metering technology.

2.2 Information Privacy Concerns

We define Internet privacy concerns as individuals' perceptions of the consequences of sharing information through the Internet (Dinev & Hart, 2006). For our purposes here, we evaluate the various infrastructure elements that convey information as though they were simply the Internet regardless of whether they are the Internet Protocol (IP) environment or other transmission media (e.g., the power line infrastructure). The various privacy concerns of users on the Internet are similar to the concerns that consumers of electricity may perceive when presented with the choice to adopt smart meters. For a thorough examination of the extant studies on information privacy concerns, see Bélanger and Crossler's (2011) literature review.

Researchers have conceptualized information privacy concerns in two widely accepted forms: concern for information privacy (CFIP) (Smith, Milberg, & Burke, 1996) and Internet users' information privacy concerns (IUIPC) (Malhotra, Kim, & Agarwal, 2004). While research on information privacy concerns has used CFIP more, other research has shown IUIPC to explain more variance in related dependent variables, such as willingness to share information online (Bélanger & Crossler, 2011). Because IUIPC is theoretically more parsimonious than CFIP and provides higher explanatory power, we use this conceptualization of information privacy concerns in our study.

The relationship between IUIPC and behavioral intention rests on the trust-risk model (McKnight, Cummings, & Chervany, 1998) and the theory of reasoned action (Fishbein & Ajzen, 1975). With regard to the trust-risk model, prior research on information privacy has shown that trust and risk are the two most prominent individual beliefs that shape the tendency to share personal information (Milne & Rohm, 2000; Miyazaki & Fernandez, 2000; Sheehan & Hoy, 2000). In the SMT context, trusting beliefs refer to the degree to which consumers believe that their utility company is reliable in guarding their personal information about electricity consumption (Gefen, Karahanna, & Straub, 2003; Grazioli & Jarvenpaa, 2000). Similarly, we define risk beliefs as perceptions that the release of personal information to a utility company will expose it to potential data loss or misuse (Dowling & Staelin, 1994). Drawing on this framework, we model information privacy concerns related to electricity consumption data as having a positive effect on risk beliefs and a negative effect on trusting beliefs. Additionally, as individuals perceive their utility companies as being trustworthy with their data, their beliefs about the risk associated with sharing electricity consumption data with the utility companies will dissipate. Thus, we hypothesize:

> **H2:** Information privacy concerns negatively influences trusting beliefs.
>
> **H3:** Information privacy concerns positively influences risk beliefs.
>
> **H4:** Trusting beliefs negatively influences risk beliefs.

In the theory of reasoned action (TRA), behavioral intention is a consistent predictor of actual behavior (Ajzen & Fishbein, 1980). IS research extensively uses behavioral intention as a proxy for actual behavior when one cannot capture actual behavior or, as in many information security studies, the behavior in question is socially undesirable. In the SMT context, behavioral intention is appropriate because of the limited rollout of SMT in most U.S. utility markets. Many consumers have not yet faced the decision of whether to adopt SMT, and, therefore, one cannot yet identify their actual behavior about adopting SMT.

Previous studies have shown that trusting beliefs and risk beliefs directly affect behavioral intention to adopt ICT (Jarvenpaa, Tractinsky, & Vitale, 2000; McKnight et al., 1998). In instances that feature SMT as the focal ICT, the more individuals trusts their utility companies with their electricity consumption data, the more likely they will be to adopt SMT. Alternatively, if individuals perceive a greater risk associated with sharing electricity consumption data, they will be resistant to accepting SMT as an adequate solution for utility management. Thus, following the IUIPC model, we hypothesize:

H5: Trusting beliefs positively influence behavioral intention to adopt smart metering technology.

H6: Risk beliefs negatively influence behavioral intention to adopt smart metering technology.

2.3 Psychological Ownership of Information

Another key element in the present study is the perceived psychological ownership of information, which we define as a mental state in which individuals perceive that the target of ownership belongs to them (Pierce, Rubenfeld, & Morgan, 1991). People may feel a sense of ownership of materials such as property or automobiles, but these feelings are not restricted to tangible objects (Dittmar, 1992). Perceptions of ownership may also extend to concepts, innovative activities, and artistic endeavors. Although research in the area of psychological ownership began in psychology, management scholars have expanded this research to the framework of organizational behavior (Pierce & Furo, 1990; Pierce, Kostova, & Dirks, 2001; Pierce, O'Driscoll, & Coghlan, 2004; Pierce et al., 1991; Van Dyne & Pierce, 2004). Because we focus on home electricity usage, we believe that the concept of psychological ownership may offer a unique avenue for exploring privacy perceptions related to information about the usage of electricity.

Psychological ownership comprises both cognitive and affective processes (Pierce et al., 2001). An individual's cognitive perception relates to that individual's cognizance, beliefs, and opinions with regard to the target of ownership, and it is shaped concurrently by the emotional connection to that target. The affective element of ownership may appear when a third party threatens perceptions of personal ownership (Pierce, Kostova, & Dirks, 2003). Perceptions of ownership can also produce feelings of pleasure (Heidegger, 1967). These cognitive and affective processes form the basis of conceptually separating psychological ownership from legal ownership (Isaacs, 1933). Because we examine the psychological ownership of information that either a utility company or consumer may legally own, we consider the connections formed by the cognitive and affective processes that result from the perception of psychological ownership.

Psychological ownership fulfills three basic human needs: self-identity, efficacy and effectance, and the sense of place (Pierce et al., 2001). In self-identity, part of the cognitive process associated with experiencing psychological ownership is to regard the target of ownership as an extension of one's self and as part of one's identity (Dittmar, 1992). One views oneself as part of the target. If one feels a great degree of psychological ownership of one's electricity usage data, one may feel that the unauthorized use of that data is a personal violation or an invasion of privacy. Efficacy and effectance refer to an owner's ability to control a target and its surrounding environment (Pierce et al., 2003). A person who experiences high levels of psychological ownership tends to feel a greater sense of efficacy because ownership increases perceptions of control and authority over both physical and non-physical targets. For example, owning a "muscle car" may facilitate feelings of control and authority in some individuals. The sense of place refers to a person's desire to assert ownership of a specific space to fulfill the psychological need to have a home (Porteous, 1976). By occupying a space, the individual identifies with it as a piece of the self, similar to self-identity. This "home" may be a variety of spaces, such as a house, a neighborhood, or a place of business.

The context of sharing information about the usage of electrical devices in a home maps particularly well with the basic needs that psychological ownership fulfills. Individuals may view their actions in the home as expressions of their self-identity. Being a homeowner also offers one a greater sense of control over one's environment. Perhaps most obviously, an individual's home also fulfills the individual's sense of place. Because a smart meter monitors the activities that occur in the home, the sharing of this information could violate any basic need that one satisfies through psychological ownership. If one perceives a high degree of psychological ownership of one's information about electricity usage, concerns related to the violation of the privacy of that information will increase. Thus, we hypothesize:

H7: Psychological ownership of electricity usage information positively influences information privacy concerns.

In addition to satisfying individuals' psychological needs, research has shown psychological ownership to have positive effects on an individual's sense of responsibility for the target of ownership. By merely perceiving the ownership of a target, an individual will possess the innate desire both to protect the target and to minimize any risks that may be associated with it (Beggan, 1992; Furby, 1978). This concept relates directly to the individual's perceptions of the risk beliefs associated with personal information. The individual's sense of responsibility toward the information about the usage of electricity due to high perceptions of psychological ownership will result in elevated perceptions of the risk beliefs associated with the sharing of such information. Thus, we hypothesize:

> **H8:** Psychological ownership of information about electricity usage positively influences risk beliefs.

2.4 Perceived Benefits and Costs

Researchers have used rational choice theory (RCT) to examine how individuals make decisions based on comparing the costs and benefits of each choice they face. Because of its action-specific nature, researchers in many fields (e.g., psychology, sociology, sociology, criminology, and economics) have applied and adapted the theory. In RCT, the process of rational thought involves recognizing different action sequences and evaluating the probable outcomes of each action sequence (Paternoster & Pogarsky, 2009). Each course of action may have multiple potential outcomes, and individuals may have different predispositions for those outcomes. An individual cognitively assigns perceived costs and/or benefits to each action based on the amount of pleasure or displeasure associated with the outcome of the action (McCarthy, 2002). The rational thought process concludes when the individual weighs the perceptions of the costs and benefits of each action sequence and selects the most appropriate choice to maximize the net pleasure gained. RCT has been applied in various information security studies (Bulgurcu, Cavusoglu, & Benbasat, 2010; Willison, 2004; Willison & Backhouse, 2006). By using the RCT's cognitive process, we can better provide key insights into individuals' decisions about whether to adopt SMT.

The specific costs and benefits associated with adopting SMT manifest through program discounts offered by the utility company, smart meter invasiveness, and the usage data's susceptibility to being shared with parties other than the utility company. To encourage consumers to adopt smart meters, some utility companies offer program discounts, such as on monthly bills, as incentives for early adopters. If a consumer perceives that the monetary benefit of adopting smart meters outweighs its perceived costs, the consumer will be more likely to adopt the SMT at home. Thus, we hypothesize:

> **H9:** Program discounts positively influences behavioral intention to adopt smart metering technology.

One of the major costs that a consumer must evaluate before choosing to adopt smart meters is the level of detail regarding the usage data that the smart meter or the various smart devices in the home would capture. We use the term meter invasiveness to refer to the amount of detail that such devices can record and how much control they possess. Some smart meters simply record the overall electricity usage in the home at the meter level, while other homes may be equipped with smart devices that can capture usage data at the device level. Further, some implementations of smart meters allow the electric utility company to power down certain devices in a home that may be consuming substantial amounts of electricity. Consumers will negatively view the increased level of scrutiny and possibly control by their electric company. Thus, we hypothesize:

> **H10:** Meter invasiveness negatively influences behavioral intention to adopt smart metering technology.

Energy consumers have several additional concerns that are associated with adopting SMT: marketers' obtaining personal usage information, the government's surveilling data, and hackers' infiltrating network security controls (Murrill, Liu, & Thompson, 2012). These concerns involve who has access to the data on their electricity usage. If hackers infiltrate the smart meter network, individual consumer data may be at risk. Utility companies may be compelled to share electricity usage information with the government for regulatory purposes. Electricity utility companies may also have a monetary incentive to share electricity consumption data with marketers. Whether hackers, the government, or third party marketers can view their data, consumers will view smart meter adoption negatively if they have strong perceptions of third party access. Consumers will likely evaluate the costs and benefits associated with smart metering technology and choose to adopt it or not to adopt it based on this cognitive evaluation. Thus, we hypothesize:

> **H11:** Third party access to energy consumption information negatively influences behavioral intention to adopt smart metering technology.

In Section 3, we describe the methods we used to collect the empirical data for this study. Gregor and Klein (2014) discuss eight obstacles that scholars who test theories encounter: three concern theorizing and five concern methodological obstacles. We carefully considered each obstacle that was relevant to our work (i.e., model justification, construct definition, common method bias testing, sample limitations, and analysis of interaction effects), and we incorporated the suggestions that Gregor and Klein (2014) offer.

3 Methods

In this study, to examine the effects of ownership, information privacy concerns, trust, risk, social influence, and perceived benefits on the consumer's behavioral intention to adopt SMT, we chose the experimental factorial design with scenarios as the appropriate method. We needed to expose the respondents to scenarios because SMT is an emerging technology, and typical energy consumers do not commonly recognize it. The scenarios included situational information that provided a realistic basis for consumers to imagine the context of adopting smart meters (Klepper & Nagin, 1989). The factorial survey differs from typical scenario-based surveys because the textual elements in the scenario are experimentally varied, which produces distinct versions of the baseline scenario. This technique combines the myriad aspects provided by field surveys with the control and orthogonality provided by experimental designs (Jasso, 2006; Rossi & Anderson, 1982). Variables can be assigned to several distinct (orthogonal) levels and infused in multiple scenario versions and, thereby, produce a full factorial design of all possible combinations of these factors and their levels. This design guarantees that the levels are orthogonal and eliminates the possibility of the multi-collinearity that may exist among the predictor variables in our model (Jasso, 2006; Rossi & Anderson, 1982; Vance, Lowry, & Eggett, 2013). By exposing each respondent to several scenarios or vignettes that each have different manipulation levels embedded in the language of the scenario, we could assess the relative roles of these factors in the respondents' intentions to adopt SMT. IS research has increasingly begun to use use the factorial survey method (D'Arcy, Hovav, & Galletta, 2009; Guo, Yuan, Archer, & Connelly, 2011; Lee, Crossler, & Warkentin, 2013; Moores & Chang, 2006; Vance et al., 2013; Vance, Lowry, & Eggett, 2015), and it has become popular in studies of information security behaviors (Crossler et al., 2013; Johnston, Warkentin, McBridge, & Carter, 2016; Lee et al., Forthcoming; Siponen & Vance, 2010; Trinkle, Crossler, & Warkentin, 2014).

3.1 Experimental Controls and Procedures: the Scenario

The scenario designed for this investigation positioned the respondents in a situation in which they could accept or decline the invitation to install smart metering technologies in their homes. We manipulated our scenarios based on a set of adoption conditions that consumers may experience when facing their adoption decision. We embedded orthogonal independent variables in the scenarios as the following values that represent such adoption conditions: program discount, meter invasiveness, and data sharing (Table 1). In the scenarios, the program discount manipulation represented the respondents' being asked to choose either to participate in the program voluntarily with no compensation or to receive a discount on their utility bill as compensation for participating. Meter invasiveness represented the level of detail of the electricity usage collected by the meter technology. For example, SMT could monitor the overall electricity usage in the entire home, or it could monitor each appliance that had a device that communicates with the smart meter base. This factor also comprises the degree of control that the utility company can exercise and ranges from simply recording the usage data to selectively shutting down appliances in order to allay brownouts during heavy consumption times. The data-sharing manipulation represented the respondents' vulnerability to third parties' gaining access to electricity usage data. In the scenario, the respondents could access their consumption data without sharing the information with the utility company, or they could grant the utility company access to the usage information. The utility company could share this information with either the government or marketers. The total number of scenario versions generated was 24 (2 x 3 x 4), but we eliminated two of the versions because they were logically impossible situations (under both program-benefit manipulations, the utility company would not be able to power down appliances selectively without the consumer-sharing usage data). We exposed each respondent to three unique versions of the scenario (see Appendix A). Researchers who have conducted previous studies with the experimental factorial design have exposed participants to as many as 64 versions during one response (Jasso, 2006). Exposing our participants to only three scenarios mitigated the potential for survey fatigue.

Table 1. Scenario Manipulation Matrix

Scenario	Manipulation		
	Discount	Invasiveness	Sharing
1	Low	Low	P
2	Low	Low	U
3	Low	Low	M
4	Low	Low	G
5	Low	Medium	P
6	Low	Medium	U
7	Low	Medium	M
8	Low	Medium	G
9	Low	High	U
10	Low	High	M
11	Low	High	G
12	High	Low	P
13	High	Low	U
14	High	Low	M
15	High	Low	G
16	High	Medium	P
17	High	Medium	U
18	High	Medium	M
19	High	Medium	G
20	High	High	U
21	High	High	M
22	High	High	G

P = personal use only; U = shared with utility company; M = data available to marketers; G = data could be shared with government

3.2 Measures and Instrumentation

Following each scenario, we presented the respondents with items that measured their intention to adopt SMT and other constructs in our model. We verified the content validity of each scale by grounding our instrument in the parameters we established from reviewing the literature. We used expert panels to refine the initial scales as we describe below. After the first instructions, the participants viewed three unique versions of the scenario and then scales of behavioral intention and a manipulation check to ensure that they read and understood the scenario.

After the respondents saw each scenario and its respective measurement items, we assessed them for their perceptions of psychological ownership, information privacy concerns, trusting beliefs, risk beliefs, and social influence. We also asked them to respond to general demographic questions, including age, gender, computer experience, education level, prior experience with personal privacy invasions, and exposure to news related to information privacy violations.

In addition to the measurement scales following each scenario and at the end of the instrument, we measured the following latent constructs using multi-item scales: perceived psychological ownership, information privacy concerns, trusting beliefs, risk beliefs, social influence, and behavioral intention to adopt smart metering technology. We adapted the scales that represented social influence and behavioral intention from Venkatesh et al. (2003) to fit the present context. We adapted the scale we used to measure psychological ownership from Van Dyne and Pierce (2004). We adapted the scales we used to measure trusting beliefs and risk beliefs from Jarvenpaa et al. (2000). We adapted the scales we used to measure each IUIPC dimension (i.e., collection, control, and awareness) from Malhotra et al. (2004). We measured each item using a five-point Likert scale, and all items were fully anchored from “strongly disagree” to “strongly agree”. Appendix B shows a detailed list of the instrument items.

We followed the guidelines for minimizing common method variance (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003) and randomized the items in the instrument to mitigate the order effect. We reduced the effects of social desirability bias by ensuring the respondents’ anonymity, using randomization, and other procedural methods. We also conducted post hoc analyses, which we discuss below.

3.3 Panel and Pilot Testing

Following the initial design of our scenario versions and instrument, we conducted an expert review panel with subject-matter experts and experts in survey instrument design. The panel mostly included faculty and doctoral students with experience in quantitative analysis and research design. Subsequently, we administered a pilot study to assess the convergent and discriminant validity of our scales, which resulted in factor loadings that conformed to accepted thresholds. Because these results confirmed the validity of our scales, we made no changes to the instrument design.

3.4 Participants

To ensure the validity of the sampling frame, we required the respondents in this factorial survey to be homeowners who paid their own utility bills. We solicited 300 respondents to participate via a paid Qualtrics panel of homeowners in the United States. We chose consumers in the US instead of in other developed countries where SMT might be implemented because of their perceptions regarding the environmental benefits associated with SMT, which fundamentally differ from the perceptions of their European counterparts (see Table 7 in Section 4). Homeowners in the US are also more likely to be presented with an adoption-choice scenario by their utility companies than European consumers, whose governments typically mandate that they accept SMT initiatives. The European Union regulates SMT adoption (Xu & Lai, 2011), whereas, in the US, private utility companies presently maintain control over their own SMT adoption authority, which often leaves the decision to consumers. The opening filter question ensured that the respondents fit the criterion of being a homeowner who paid their own utility bills. Research that employs the experimental factorial design typically generates scenarios that apply to the sample population (Rossi & Anderson, 1982). After eliminating the responses caused by response set (Andrich, 1978; Kerlinger, 1973; Rennie, 1982), unreasonably short completion times, and/or failed manipulation checks, we retained 229 usable responses. We exposed each respondent to three unique versions of the scenario, which resulted in 687 responses at the vignette level.

4 Data Analysis and Results

In this section, we explain how we analyzed the data, assessed instrument validity, tested construct validity, and analyzed the conceptual model.

4.1 Instrument Validity

Because we conceptualized behavioral intention, psychological ownership, risk beliefs, trusting beliefs, and social influence as reflective, we used multi-item scales to measure them. To ensure the consistency of the items in a scale, adequate reliability must be demonstrated. We calculated composite reliability for each reflective scale. Reliability exceeded .8 for each scale, which suggests each scale’s items were sufficiently consistent (Churchill, 1979; Mackenzie, Podsakoff, & Podsakoff, 2011; Peter, 1981). One establishes convergent validity to ensure that each item that measures a particular construct significantly correlates with its construct’s composite value (Straub, Boudreau, & Gefen, 2004). The partial least squares (PLS) reports for cross-loadings showed that all constructs had significant convergent validity. We also demonstrated discriminant validity for our reflective constructs. We found cross-loadings that exceeded .40 between psychological ownership and risk beliefs. Cross-loading was also evident between social influence and trusting beliefs. Cross-loadings between all other constructs were not significant. Table 2 shows the loadings, cross-loadings, and composite reliability of all reflective scale items. We also examined convergent and discriminant validity by comparing shared variances between constructs with the average variance extracted (AVE) of the respective constructs (Fornell & Larcker, 1981). The AVE of each construct should exceed .5, and the shared variance between constructs should not exceed either of the constructs’ AVEs. Although we found some cross-loading between constructs, the AVE of each construct exceeded .5 and was greater than any variance shared with other constructs. Table 3 shows the shared variances and AVEs of each construct.

Table 2. Loadings and Cross-loadings for Reflective Constructs

	BI	OWN	RB	SI	TB	Composite reliability
BI1	**.973**	-.114	-.257	.342	.355	.984
BI2	**.975**	-.101	-.267	.363	.373	
BI3	**.980**	-.105	-.258	.357	.361	
OWN1	-.134	**.843**	.544	-.259	-.235	.869
OWN2	-.028	**.786**	.472	-.141	-.068	
OWN3	-.098	**.820**	.462	-.200	-.128	
OWN4	-.081	**.703**	.460	-.073	-.109	
RB1	-.228	.448	**.848**	-.096	-.292	.926
RB2	-.212	.485	**.835**	-.138	-.397	
RB3	-.251	.547	**.838**	-.227	-.332	
RB4	-.181	.533	**.840**	-.110	-.277	
RB5	-.250	.579	**.866**	-.198	-.333	
SI1	.254	-.148	-.059	**.768**	.317	.896
SI2	.354	-.225	-.255	**.907**	.510	
SI3	.207	-.127	.022	**.723**	.309	
SI4	.351	-.198	-.230	**.897**	.436	
TB1	.350	-.143	-.332	.426	**.843**	.910
TB2	.342	-.197	-.379	.478	**.883**	
TB3	.326	-.152	-.351	.337	**.831**	
TB4	.250	-.029	-.211	.344	**.727**	
TB5	.220	-.153	-.267	.398	**.802**	

Table 3. Loadings and Cross-loadings for Reflective Constructs

	Mean	Std. dev.	BI	OWN	RB	SI	TB
BI	3.022	1.234	(.953)				
OWN	3.625	0.699	.012	(.624)			
RB	3.258	0.833	.071	.378	(.715)		
SI	2.985	0.787	.132	.047	.034	(.685)	
TB	3.247	0.717	.138	.030	.150	.238	(.671)
AVEs are shown in parentheses. BI = behavioral intention, OWN = psychological ownership, RB = risk beliefs, SI = social influence, TB = trusting beliefs.							

4.2 Common Method Bias

We also conducted a post hoc analysis to detect whether common method bias (i.e., common methods variance) posed a significant risk to our interpretation of the data. Because we used partial least squares (PLS) to analyze the relationships hypothesized in the research model, using an unmeasured latent method construct (ULMC) to analyze the common-method bias post hoc was not appropriate (Chin, Thatcher, & Wright, 2012). However, because it uses maximum likelihood calculations, the ULMC test is appropriate to use to detect common method bias (Marsh & Hocevar, 1988; Straub et al., 2004; Woszczynski & Whitman, 2004).

We administered the ULMC test with AMOS version 23. This analysis compares the $\chi 2$ score of the native measurement model to the $\chi 2$ score of a measurement model that includes a ULMC correlated with all measurement items, which results in a difference in degrees of freedom between models equal to one.

For there to be a significant difference in the model fit between two models that differ by only one degree of freedom, the difference in $\chi 2$ must be greater than or equal to 3.84. The $\chi 2$ difference test indicated that common method bias did not have a significant effect on this dataset ($\chi 2$ = 1277.970 with common-method factor included; $\chi 2$ = 1280.209 without common-method factor; $\chi 2$ difference = 2.239).

4.3 PLS Analysis

We tested the structural model and its associated hypotheses using SmartPLS (Ringle, Wende, & Will, 2005). In addition, we used a bootstrapping resampling technique, which approximates the path coefficients and the amount of variance explained in mediating variables. With the exception of H9, we found support for all hypotheses. In comparison to previous research that has examined technology adoption and privacy and security concerns, the amount of variance explained by the model we used was acceptable (Chan et al., 2010; Liang & Xue, 2010; Wang & Benbasat, 2005). Table 4 shows the overall findings.

As Figure 2 illistrates, the model explained approximately 28.1 percent of the variance in behavioral intention, which demonstrates that the experimental data supported the research model. We discuss the insights we discovered from analyzing the data below.

Table 4. Hypothesis Support

Hypothesis (with direction)	Path coefficient (β)	T-value	P-value	Supported?
H1: SI → BI (+)	.208	5.117	p < .001	Supported
H2: IUIPC → TB (-)	-.311	5.443	p < .001	Supported
H3: IUIPC → RB (+)	.516	15.392	p < .001	Supported
H4: TB → RB (-)	-.182	6.167	p < .001	Supported
H5: TB → BI (+)	.163	3.611	p < .001	Supported
H6: RB → BI (-)	-.145	4.016	p < .001	Supported
H7: OWN → IUIPC (+)	.634	20.730	p < .001	Supported
H8: OWN → RB (+)	.256	7.490	p < .001	Supported
H9: PD → BI (+)	.047	1.386	p > .05	Not supported
H10: MI → BI (-)	-.110	3.115	p < .001	Supported
H11: TPA → BI (-)	-.211	6.326	p < .001	Supported
SI = social influence, BI = behavioral intention, IUIPC = Internet users' information privacy Concerns, TB = trusting beliefs, RB = risk beliefs, OWN = psychological ownership, PD = program discount, MI = meter invasiveness, TPA = third party access.				

Our results supported most of the hypothesized relationships. Of the significant hypotheses, our results supported them at an alpha level of 0.01 or lower. Consistent with the hypothesized relationships, social influence had a significant positive effect on behavioral intention (β = .208, $p < .001$). Information privacy concerns had a significant negative relationship with trusting beliefs (β = -.311, $p < .001$), and they positively influenced risk beliefs (β = .516, $p < .001$). Trusting beliefs negatively influenced risk beliefs (β = -.182, $p < .001$) and had a significant positive effect on behavioral intention (β = .163, $p < .001$). Psychological ownership had a significant positive influence on both information privacy concerns (β = .634, $p < .001$) and risk beliefs (β = .256, $p < .001$). Sharing electricity usage information with a third party had a significant negative effect on behavioral intention (β = -.211, $p < .001$). Our results did not support H9. The program discount did not have a significant effect on behavioral intention (β = .047, $p > .05$).

We conducted additional analyses to determine the impact of specific benefits of SMT on behavioral intention. The benefits examined included avoiding brownouts, saving money, saving the environment, having the latest technology, and having more information about monthly electricity usage. We also assessed the respondents' level of concern about hackers gaining access to electricity usage information. We included each of these variables in the PLS model, which showed that only the avoidance of brownouts had a significant effect on behavioral intention (β = .125, $p < .001$).

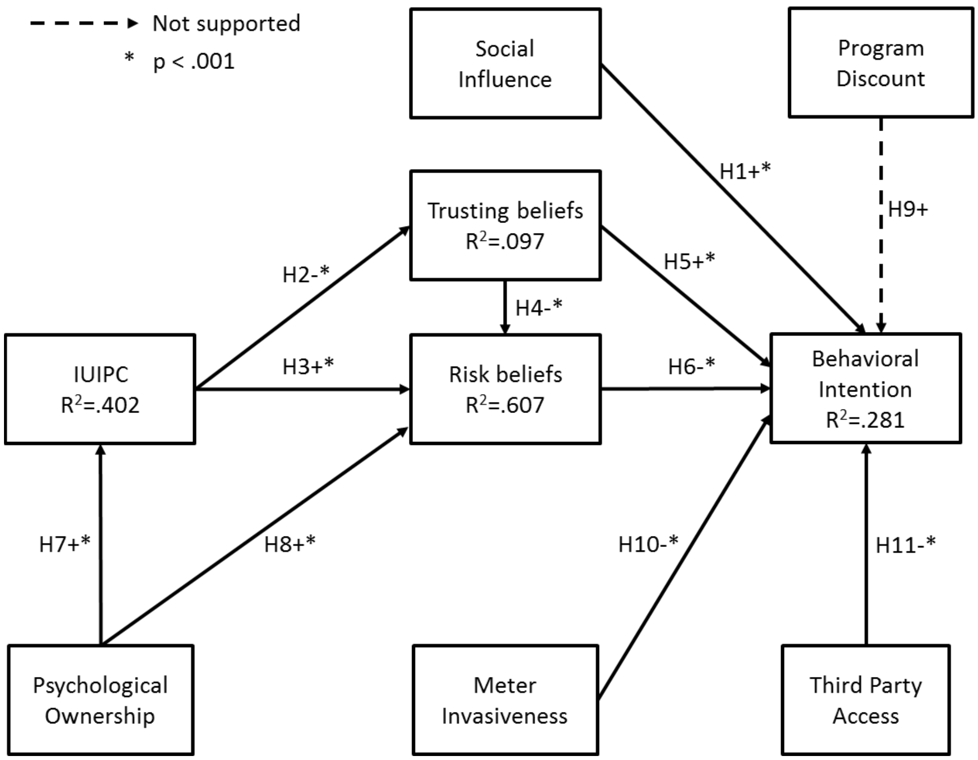

Figure 2. Results of Structural Model Analysis

Table 5. Mediation Testing for Indirect Effects

Relationship	β (IV→MV)	SE (IV→MV)	β (MV→DV)	SE (MV→DV)	T-Value	P-Value	Mediation
PO→IUIPC→RB	0.618	0.033	0.519	0.034	11.751	p < .001	Partial
PO→IUIPC→TB	0.618	0.033	-0.357	0.064	-5.369	p < .001	Full
PO→RB→BI	0.265	0.035	-0.177	0.051	-3.169	p < .001	Full
IUIPC→TB→RB	-0.357	0.064	-0.170	0.029	4.032	p < .001	Partial
IUIPC→TB→BI	-0.357	0.064	0.148	0.046	-2.807	p < .01	Full
IUIPC→RB→BI	0.519	0.034	-0.177	0.051	-3.401	p < .001	Full

β = path coefficient, SE = standard error, IV = independent variable, MV = mediator variable, DV = dependent variable, PO = psychological ownership, RB = risk belief, TB = trusting belief, BI = behavioral intention.

Because our model also contained various mediator constructs, we conducted mediation tests to determine the nature of the mediation tested and whether significant indirect effects existed. Following Baron and Kenny's (1986) guidelines for mediation testing, we used a Sobel test to assess the significance of each of the indirect effects. Table 5 describes each mediation test in detail. Each of the indirect effects depicted in our research model was significant. Psychological ownership had a positive indirect effect on risk belief through IUIPC, whereas it had a negative indirect effect on trusting beliefs through IUIPC. Because of the direct effect of psychological ownership on risk beliefs, IUIPC partially mediated this relationship. Conversely, IUIPC fully mediated the relationship between psychological ownership and trusting beliefs. Psychological ownership also had a negative indirect effect on behavioral intention through risk beliefs, which fully mediated the relationship. Trusting beliefs partially mediated IUIPC's indirect positive influence on risk beliefs. Both trusting beliefs and risk beliefs fully mediated IUIPC's indirect negative influence on behavioral intention. The results of these mediation tests confirmed the presence of the full or partial mediation depicted in the research model.

5 Discussion and Contribution

The smart grid is an important technological innovation that spans the domains of power, communication, and information technology. Although tremendous strides have been made in technology development, little attention has focused on the issues involving consumers' adopting SMT. The adoption of SMT could result in benefits for utility companies in the form of reduced operating costs and benefits for consumers in terms of lower energy bills and fewer brownouts. However, privacy concerns and consumers' perceived ownership of electricity usage information could hamper utility companies' efforts to widely implement SMT programs. Our results provide insights into consumers' perceptions of both the benefits and the concerns associated with SMT adoption and the relationship between information privacy concerns and psychological ownership in the context of smart meter technology.

5.1 Theoretical Implications

In this study, we explore the unique, emerging phenomenon of the role of shared benefits in technology adoption by applying and extending extant theories. We contextualize adoption theories in this unique phenomenon while incorporating the perspective of the perceived psychological ownership of data. We achieve this theory contextualization by explicitly articulating our boundary conditions as Sarker (2016) describes and by describing several extensions that one may realize from our contributions. Our findings provide insights that extend beyond UTAUT or IUIPC; that is, we do more than simply apply foundation theories to the new context of SMT adoption. Our results fill a gap in the literature by providing evidence of an important new factor that influences individual adoption decisions in contexts where perceived shared benefits exist. This contribution to theory, based on insights gained by exposing homeowners to various hypothetical situational variables, enables a more nuanced understanding of the factors that shape the privacy perceptions of homeowners in the US, and, to the extent that these boundary conditions are not violated, one may extend them to 1) other Western countries and 2) other technologies that may gather information about individual behaviors and actions. Of particular importance is the specific insight regarding the role of the shared benefit in this context. Our findings of the shared benefit of accepting the recommendation to adopt SMT offer an important new theoretical insight into any adoption decision in which such shared benefits may exist. For example, "lurkers" do not enhance the benefits of a social network for its members, so the contributions of the entire group increase the shared informational benefit to each member. Similarly, shared benefits accrue to society when individuals choose to vaccinate their children, conserve water, or reduce the consumption of other scarce resources. Although our findings apply directly to the SMT context, others could extend them to other adoption decisions that include shared benefits.

We assessed the respondents on their individual perceptions of the specific benefits associated with SMT. The only benefit that had a significant effect on behavioral intention was avoiding brownouts. This finding is interesting because meter invasiveness was negatively significant. Our results show that, while consumers were concerned about losing a degree of control over their appliances, they were interested in avoiding brownouts, which a utility company's selectively allocating power via smart meters mitigates. In communicating the benefits of SMT, utility companies may need to emphasize the avoidance of brownouts as a key benefit in order to convince consumers that SMT is ultimately worth adopting. They should convey that, although everyone shares the benefits, individuals need to occasionally sacrifice their household power to avoid brownouts throughout their region.

Our model explained a reasonable amount of variance in behavioral intention to adopt SMT. Social influence's effect indicates that consumers care about the perceptions and opinions of the influential people in their lives with regard to SMT adoption. This particular facet of the UTAUT model is applicable in the SMT context. The specific implementation of smart meters and the associated data-sharing policies also significant influenced behavioral intention. Meter invasiveness had a significant negative influence on behavioral intention, which shows that, as consumers cede more control and information to the utility company, they are less likely to adopt SMT. Sharing information about electricity usage with third parties had a significant negative effect on behavioral intention. The strength of the relationships between government access and marketer access regarding behavioral intention was especially strong, which indicates that, while consumers are apprehensive about sharing usage information with their utility companies, they may be even more cautious about doing so when it is possible that they would share information with the government or marketers.

As the leading theorization literature has called for, we contextualize the extant theories by focusing on this new phenomenon. We found strong support for the IUIPC model in the SMT context. As expected, trusting beliefs and risk beliefs had a significant effect on behavioral intention. The addition of psychological ownership in our model has interesting theoretical implications for the amount of variance explained in both IUIPC and risk beliefs. Although a high degree of correlation may typically be cause for concern when analyzing latent constructs (R^2 of IUIPC = 40.2%; R^2 of risk beliefs = 60.7%), traditionally, IUIPC has shown a high degree of correlation with risk beliefs (usually R^2 ~50%; Malhotra et al., 2004). Despite the high inter-construct correlation, researchers widely consider these constructs to be theoretically related but distinct. Our theoretical arguments and data analysis demonstrate that psychological ownership was indeed distinct from both IUIPC and risk beliefs but that they were theoretically closely related. Our model also demonstrates that psychological ownership partially mediated IUIPC and risk beliefs in that it had both direct and indirect effects on risk beliefs through IUIPC. Psychological ownership is an important addition to the traditional IUIPC model considering the potential violation of private information that is closely tied to self-identity, sense of control, and sense of home.

5.2 Practical Implications

Our findings can inform policy makers about some key concerns of potential smart grid users: 1) physical intrusions into their homes by criminals who discern opportune times to break in by analyzing smart meter data, 2) hackers' ability to control appliances in households, 3) personal data's being commercially misused if utility companies sell consumption information to third parties, 4) government intrusion into their private lives, 5) discrimination in health insurance and employment based on revelations of lifestyle choices, 6) a barrage of marketing based on revelations of lifestyle choices through metering data, and 7) a loss of control of electricity usage. Each of these concerns requires a thorough investigation by behavioral scientists.

The data collected by smart meters raises questions of privacy and ownership. The primary concern is that the data may not be adequately protected and that others (e.g., hackers, businesses, and intelligence organizations) might be able to obtain it to gather information about consumers' lifestyles and behaviors (Goel, 2015). Law enforcement may need to track the behavior and daily routine of an individual during a crime investigation. We need clear public policy to address consumers' concerns about the potential for law enforcement agencies to intrude on individuals' privacy via smart meter data. Our results provide the foundation for a public policy on smart grid privacy.

Our study also has important implications for the role of utilities in improving adoption. One of the most sensitive issues related to SMT adoption involves the right to exploit consumers' usage data for commercial purposes. To address the concerns of consumers, utility companies will need to work with regulators to define how energy data can and cannot be used. Parallels can be drawn with the experience of the telecommunications industry in allowing the usage of phone data, which is also sensitive and reveals information about personal habits and lifestyle choices.

Another key area of public policy to which our findings pertain concerns incentives and mandates. Our study contributes to our understanding of the multifaceted reasons for why individuals resist adopting SMT and value propositions based on pricing incentives for energy shifting. Currently, the only value proposition for consumers is avoiding brownouts, which outweighed the invasiveness and anticipated cost of smart meters. Our findings establish a baseline for understanding consumer concerns regarding the adoption of SMT.

6 Limitations and Future Research

By initially establishing our theory's boundary conditions (see Section 1), we may have limited the generalizability of our findings in certain ways. Sarker (2016) suggests that a balance between generality and contextual specificity may result from multiple studies. We specifically targeted the discrete context of SMT adoption decisions, and we investigated this phenomenon with a survey that leveraged constructs from core theories that we adapted to this context. Future studies may facilitate greater generalizability of our findings.

Although we found good support for our model overall, we did not find support for one hypothesis. Program discounts, such as offering a discount on monthly bills to incentivize participation, did not significantly affect behavioral intention to adopt SMT. This finding may indicate that a 10 percent discount (as we described in the scenario) is not sufficient to convince consumers to adopt SMT. This interesting result supports previous studies that have found that an economic benefit was a necessary, but insufficient, motivator for altering consumer behavior in energy conservation (Baddeley, 2011). Future studies on SMT may find it beneficial to increase the variability in manipulating program discount, such as greater discounts, to determine whether a threshold beyond which the financial effect would motivate behavior change exists.

One could extend our research by examining differences in SMT adoption intentions based on political affiliation. Previous research has found that liberals' views on climate change tended to align with the findings of studies of global climate change. Conservatives tended to be skeptical of scientific research and tended to disagree with these findings (Mccright & Dunlap, 2011). Individuals' political leanings may affect their perceptions of the climatological risks associated with energy consumption. Because ideology could have a significant influence on adoption intentions, it could be interesting avenue for future research.

Another opportunity for future research would be to adapt our model to other contexts similar to SMT, such as the adoption of event data recorders (EDR), which capture data on drivers' behavior in automobiles. Although unique facets contribute to the SMT context, concerns about the privacy of information and the psychological ownership of data remain relevant. EDR and similar technologies that capture user behaviors fit the boundary conditions identified in our contextualization process.

Another potentially fruitful area for expanding the theory in this domain would involve exploring adoption resistance that a perceived loss of control causes. One could incorporate the construct "perceived behavioral control" (Ajzen & Madden, 1986) into the model to explore how this factor might change the decision calculus. Ajzen (2002) found measurement and other concerns in operationalizing this construct and that self-efficacy (related to perceived difficulty) and controllability (perceived influence on performance) exhibited sufficient commonality and might not be independent of each other as is widely accepted. Despite such controversy, we urge future researchers to explore this facet of the process used in deciding to adopt smart meters.

Our findings contribute to the theoretical and practical understanding of issues related to sustainability. Because most green initiatives include impact on society and the planet, future adoption research that examines the effects on sustainability should include the concept of shared benefits of technology adoption. Our study also addresses the recent call for research that offers concrete, practical conclusions and theoretical contributions for green IS issues (Gholami et al., 2016).

Information privacy continues to be a widely discussed area of research, especially as smart devices become ubiquitous in consumers' lives. However, users may have concerns about the type of data that various smart devices collect. Determining consumers' greatest concerns about the collection of information about electricity usage and creating measures to protect such data will help foster the adoption of SMT. Implementing fair usage policies and communicating these procedures to energy consumers should alleviate customers' fears and empower them to learn about the potential risks and benefits of adopting smart meters. Emphasis on the avoidance of brownouts or rolling blackouts may also be helpful in convincing energy consumers that SMT is truly beneficial and worthwhile. In addition, creating privacy protocols that camouflage individual usage by either aggregation or obfuscation would help improve consumers' confidence with respect to their privacy. Related to this concern would be studies on the consequences of privacy-invasive technologies. We foresee an opportunity to contribute a nuanced understanding of the implications for privacy of this phenomenon, which future research projects designed to measure the perceived consequences of privacy-invasive practices could offer. Beyond understanding individual concerns regarding privacy, we need to develop models to explore the various ways in which the privacy-invasive monitoring of appliance activity, for example, could influence various responses by individuals in the home, including the resulting changes in usage behaviors.

7 Conclusions

A plethora of research has focused on factors that research has shown to influence individual adoption decisions, including the traditional UTAUT variables and the rational assessment of costs and benefits. This study represents the first in the IS adoption literature to investigate the role of a shared benefit in the adoption decision. The IS research community lacks empirical evaluations of the role (as a decision driver) of the benefits that accrue to society in contexts of technology adoption where this possibility exists. Our results fill this gap in the research. We also contextualize and validate the extant adoption theories in the context of a unique voluntary adoption decision (SMT) and an emerging technology that presents unique privacy factors to the decision maker. Finally, this study also contributes to our understanding of the role of the perceived psychological ownership of data, which is a salient factor in adoption decisions that affect users' privacy.

References

Adger, N. (2003). *Social capital, collective action, and adaptation to climate change*. Economic Geography, *79*(4), 387-404.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665-683.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour.* Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology*, *22*(5), 453-474.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Andrich, D. (1978). A rating formulation for ordered response categories. *Psychometrika*, *43*(4), 561-573.

Baddeley, M. (2011). *Energy, the environment and behaviour change: A survey of insights from behavioural economics* (No. CWPE 1162). University of Cambridge.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems*, *8*(4), 244-254.

Bamberger, P. (2008). From the editors: Beyond contextualization: Using context theories to narrow the micro-macro gap in management research. *Academy of Management Journal, 51*(5), 839-849.

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

Beggan, J. K. (1992). On the social nature of nonsocial perceptions: The mere ownership effect. *Journal of Personality and Social Psychology*, *62*(2), 229-237.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041.

Breward, M., Hassanein, K., & Head, M. (Forthcoming). Understanding consumers' attitudes toward controversial information technologies: A contextualization approach*. Information Systems Research.*

Brooks, S., Wang, X., & Sarker, S. (2012). Unpacking green IS: A review of the existing literature and directions for the future. In J. vom Brocke, S. Seidel, & J. Recker (Eds.), *Green business process management* (pp. 15-37). Berlin, Heidelberg: Springer.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security Awareness. *MIS Quarterly*, *34*(3), 523-548.

Califf, C., Lin, X., & Sarker, S. (2012). Understanding energy informatics: A gestalt-fit perspective. In *Proceedings of the Americas Conference on Information Systems.*

Cappelli, P., & Sherer, P. D. (1991). The missing role of context in OB—the need for a meso-level approach. *Research in Organizational Behavior*, *13*, 55-110.

Chan, F. K. Y., Thong, J. Y. L., Venkatesh, V., Brown, S. A., Hu, P. J., & Tam, K. Y. (2010). Modeling citizen satisfaction with mandatory adoption of an e-government technology. *Journal of the Association for Information Systems*, *11*(10), 519-549.

Cheung, C. M. K., Lee, M. K. O., & Rabjohn, N. (2008). The impact of electronic word-of-mouth. *Internet Research*, *18*(3), 229-247.

Chin, W. W., Thatcher, J. B., & Wright, R. T. (2012). Assessing common method bias: Problems with the ULMC technique. MIS Quarterly, 36(3), 1003-1019.

Chu, S.-C. (2009). *Determinants of consumer engagement in electronic word-of-mouth in social networking sites.* University of Texas at Austin.

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

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*(1), 90-101.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Darby, S. (2010). Smart metering: What potential for householder engagement? *Building Research & Information*, *38*(5), 442-457.

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

Dittmar, H. (1992). *The social psychology of material possessions: To have is to be.* New York: St. Martin's Press.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research*, *21*(1), 119-134.

Fichman, R. G. (2000). The diffusion and assimilation of information technology innovations. In R. W. Zmud (Ed.), *Framing the Domains of IT Management: Projecting the future…through the* past (pp. 105-127). Cincinnati, OH: Pinnaflex Education Resources.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement Error. *Journal of Marketing Research*, *18*, 39-50.

Fridgen, G., Häfner, L., König, C., & Sachs, T. (2016). Providing utility to utilities: The value of information systems enabled flexibility in electricity consumption. *Journal of the Association for Information Systems*, *17*(8), 537-563.

Furby, L. (1978). Possession in humans: An exploratory study of its meaning and motivation. *Social Behavior and Personality*, *6*(1), 49-65.

Gatignon, H., & Robertson, T. S. (1989). Technology diffusion: An empirical test of competitive effects. *Journal of Marketing*, *53*, 35-49.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51-90.

Geroski, P. (2000). Models of technology diffusion. *Research Policy*, *29*(4-5), 603-625.

Gholami, R., Watson, R. T., Hasan, H., Molla, A., & Bjørn-Andersen, N. (2016). Information systems solutions for environmental sustainability: How can we do more? *Journal of the Association for Information Systems*, *17*(8), 521-536.

Goel, S. (2015). Anonymity vs. security: The right balance for the smart grid. *Communications of the AIS*, *36*, 23-32.

Goel, S., Bush, S. F., & Neuman, C. (2013). Smart grid security. In S. Goel, S. F. Bush, & D. Bakken (Eds.), *IEEE vision for smart grid communications: 2030 and beyond* (pp. 271-296). *IEEE.*

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished: Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18(*1), 22-44.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Management, and Cybernetics, Part A: Systems Humans*, *30*(4), 395-410.

Gregor, S., & Klein, G. (2014). Eight obstacles to overcome in the theory testing genre. *Journal of the Association for Information Systems*, *15*(11), i-xix.

Guo, K., Yuan, Y., Archer, N., & Connelly, C. (2011). Understanding non-malicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Gupta, A. (2012). Consumer adoption challenges to the smart grid. *Journal of Service Science*, *5*(2), 79-86.

Heidegger, M. (1967). *Being and time* (J. Macquarrie & E. Robinson, trans.). Oxford: Blackwell.

Hess, D. J., & Coley, J. S. (2012). Wireless smart meters and public acceptance: The environment, limited choices, and precautionary politics. *Public Understanding of Science*, 1-15.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*(1), 111-136.

Huang, Z., & Palvia, P. (2016). Consumers' privacy concerns about smart meters. In *Proceedings of the 22nd Americas Conference on Information Systems.*

Isaacs, S. (1933). *Social development in young children*. London: Routledge and Kegan Paul.

James, T. L., Nottingham, Q., Collignon, S. E., Warkentin, M., & Ziegelmayer, J. (2016). The interpersonal privacy identity (IPI): Development of a privacy as control model. *Information Technology and Management*, *17*(4), 341-360.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management*, *1*, 45-71.

Jasso, G. (2006). Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research*, *34*(3), 334-423.

Johns, G. (2006). The essential impact of context on organizational behavior. *Academy of Management Review*, *31*(2), 386-408.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. D. (2016). Dispositional and situational factors: Influences on IS security policy violations. *European Journal of Information Systems*, *25*(3), 231-251.

Joshi, A., & Roh, H. (2009). The role of context in work team diversity research: a meta-analytical review. *Academy of Management Journal*, *52*(3), 599-627.

Kahneman, D. (2012). A proposal to deal with questions about priming effects. *Nature*.

Kerlinger, F. N. (1973). *Foundations of behavioral research* (3rd ed.). London, UK: Holt, Rinehart & Winston.

Klepper, S., & Nagin, D. (1989). The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology*, *27*(4), 721-746.

Kostyk, T., & Herkert, J. (2012). Societal implications of the emerging smart grid. *Communications of the ACM*, *55*(11), 34-36.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research*, *14*(3), 221-243.

Lee, A. S., & Baskerville, R. L. (2012). Conceptualizing generalizability: New contributions and a reply. *MIS Quarterly*, *36*(3), 749-761.

Lee, J., Crossler, R. E., & Warkentin, M. (2013). Implications of monitoring mechanisms on bring your own Device (BYOD) adoption. In *Proceedings of the 34th International Conference on Information Systems.*

Lee, J., Jr., Crossler, R. E., Otondo, R., & Warkentin, M. (Forthcoming). Implications of monitoring mechanisms on bring your own device adoption. *Journal of Computer Information Systems*.

Lei, C. F., & Ngai, E. W. T. (2013). Green IT adoption: An academic review of literature. In *Proceedings of the Pacific Asia Conference on Information Systems.*

Li, X. (2004). Informational cascades in IT adoption. *Communications of the ACM*, *47*(4), 93097.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413.

Lu, J., Yu, C.-S., Liu, C., & Yao, J. E. (2003). Technology acceptance model for wireless Internet. *Internet Research*, *13*(3), 206-222.

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293-334.

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.

Marsh, H. W., & Hocevar, D. (1988). A new, more powerful approach to multitrait-multimethod analyses: Application of second-order confirmatory factor analysis. *Journal of Applied Psychology*, *73*(1), 107-117.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*, *28*(1), 417-442.

Mccright, A. M., & Dunlap, R. E. (2011). The politicization of climate change and polarization in the American public's views of global warming, 2001-2010. *Sociological Quarterly*, *52*(2), 155-194.

McKenna, E., Richardson, I., & Thomson, M. (2012). Smart meter data: Balancing consumer privacy concerns with legitimate applications. *Energy Policy*, *41*, 807-814.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *The Academy of Management Review*, *23*(3), 473-490.

Milne, G. R., & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing*, *19*(2), 238-249.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, *19*(1), 54-61.

Moores, T., & Chang, J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly*, *30*(1), 167-180.

Murrill, B., Liu, E., & Thompson II, R. (2012). *Smart meter data: Privacy and cybersecurity.* CRS Report for Congress.

Okazaki, S. (2005). New perspectives on m-commerce research. *Journal of Electronic Commerce Research*, *6*(3), 160-164.

Olbrich, S., Frank, S., Gregor, S., Niederman, F., & Rowe, F. (2016). On the merits and limits of replication and negation for IS research. *AIS Transactions on Replication Research, 3,* 1-19.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology*, *25*(2), 103-127.

Peter, J. P. (1981). Construct validity: A review of basic issues and marketing practices. *Journal of Marketing Research*, *18*(2), 133-145.

Pierce, J. L., & Furo, C. A. (1990). Employee ownership: Implications for management. *Organizational Dynamics*, *18*(3), 32-43.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2001). Toward a theory of psychological ownership in organizations. *Academy of Management Review*, 2*6*(2), 298-310.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology*, *7*(1), 84-107.

Pierce, J. L., O'Driscoll, M. P., & Coghlan, A.-M. (2004). Work environment structure and psychological ownership: The mediating effects of control. *The Journal of Social Psychology*, *144*(5), 507-534.

Pierce, J. L., Rubenfeld, S. A., & Morgan, S. (1991). Employee ownership: A conceptual model of its processes and effects. *Academy of Management Review*, *16*(1), 121-144.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879-903.

Porteous, J. D. D. (1976). Home: The territorial core. *Geographical Review*, *66*(4), 383-390.

Potter, C. W., Archambault, A., & Westrick, K. (2009). Building a smarter smart grid through better renewable energy information. In *Proceedings of the IEEE/PES Power Systems Conference and Exposition.*

Rennie, L. (1982). Research note: Detecting a response set to Likert-style attitude items with the rating model. *Educational Research and Perspectives*, *9*(1), 114-118.

Ringle, C. M., Wende, S., & Will, A. (2005). *SmartPLS.* Hamburg, Germany: SmartPLS.

Rossi, P. H., & Anderson, A. B. (1982). The factorial survey approach: An introduction. In P. H. Rossi & S. L. Nock (Eds.), *Measuring social judgments* (pp. 15-67). Beverly Hills, CA: Sage.

Salovaara, A., & Merikivi, J. (2015). IS research progress would benefit from increased falsification of existing theories. In *Proceedings of the European Conference on Information Systems*.

Sarker, S. (2016). Building on Davison and Martinsons' concerns: a call for balance between contextual specificity and generality in IS research. *Journal of Information Technology*, *31*(3), 250-253.

Seddon, P. B., & Scheepers, R. (2012). Towards the improved treatment of generalization of knowledge claims in IS research: Drawing general conclusions from samples. *European Journal of Information Systems*, *21*(1), 6-21.

Seddon, P. B., & Scheepers, R. (2015). Generalization in IS research: A critique of the conflicting positions of Lee & Baskerville and Tsang & Williams. *Journal of Information Technology*, *30*(1), 30-43.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, *19*(1), 62-73.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-502.

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

Straub, D. W., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the AIS*, *13*, 381-427.

Systems, S., McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security Privacy Magazine*, *7*(3), 75-77.

Trinkle, B. S., Crossler, R. E., & Warkentin, M. (2014). I'm game, are you? reducing real-world security threats by managing employee activity in virtual environments. *Journal of Information Systems*, *28*(2), 307-327.

Van Dyne, L., & Pierce, J. L. (2004). Psychological ownership and feelings of possession: three field studies predicting employee attitudes and organizational citizenship behavior. *Journal of Organizational Behavior*, *25*(4), 439-459.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263-289.

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to address the problem of access-policy violations. *MIS Quarterly*, *39*(2), 345-366.

Venkatesh, V., Morris, M. G., Davis, G. B., Davis, F. D., & Hall, M. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425-478.

Wang, W., & Benbasat, I. (2005). Trust in and adoption of online recommendation agents. *Journal of the Association for Information Systems*, *6*(3), 72-101.

Wang, X., Brooks, S., & Sarker, S. (2015a). A review of green IS research and directions for future studies. *Communications of the Association for Information Systems*, *37*, 395-492.

Wang, X., Brooks, S., & Sarker, S. (2015b). Understanding green IS initiatives: A multi-theoretical framework. *Communications of the AIS*, *37*, 670-704.

Watson, R. T., Boudreau, M.-C., & Chen, A. J. (2010). Information systems and environmentally sustainable development: Energy informatics and new directions for the IS community. *MIS Quarterly*, *34*(1), 23-38.

Whetten, D. A. (2009). An examination of the interface between context and theory applied to the study of Chinese organizations. *Management and Organization Review*, *5*(1), 29-55.

Whetten, D. A., Felin, T., & King, B. G. (2009). The practice of theory borrowing in organizational studies: Current issues and future directions. *Journal of Management*, *35*(3), 537-563.

Willison, R. (2004). Understanding the offender/environment dynamic for computer crimes: Assessing the feasibility of applying criminological theory to the IS security context. In *Proceedings of the 37th Hawaii International Conference on System Science*s (pp. 1-10).

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems*, 15(4), 403-414.

Woszczynski, A. B., & Whitman, M. E. (2004). The problem of common method variance in IS research. In A. B. Woszczynski & M. E. Whitman (Eds.), *The handbook of information systems research* (pp. 66-77). Hershey, PA: Idea Group Publishing.

Wunderlich, P., Veit, D., & Sarker, S. (2012a). Adoption of information systems in the electricity sector: The issue of smart metering. In *Proceedings of the Americas Conference on Information Systems.*

Wunderlich, P., Veit, D., & Sarker, S. (2012b). Examination of the determinants of smart meter adoption: An user perspective. In *Proceedings of the 33rd International Conference on Information Systems*.

Xu, F. Y., & Lai, L. L. (2011). Scope design, charateristics and functionalities of smart grid. In *Proceedings of the IEEE Power and Energy Society General Meeting.*

Xu, X., Venkatesh, V., Tam, K. Y., & Hong, S.-J. (2010). Model of migration and use of platforms: Role of hierarchy, current generation, and complementarities in consumer settings. *Management Science*, *56*(8), 1304-1323.

Appendix A: Scenario Construction

Baseline Scenario

In this scenario, please assume that your electric utility company has **[program discount manipulation]** to participate in a new program. Under this program, **[metering invasiveness manipulation]**. **[data sharing manipulation].**

Manipulation Statements

Program Discount

1. Asked if you would volunteer
2. Offered you a discount on your monthly bill

Metering Invasiveness

1. A new meter will be installed inside your home, allowing you to monitor your home's electricity usage in real time, but your appliances will not be fitted to communicate with the meter.
2. You will have a smart meter installed at your home, and all of your appliances will be fitted to communicate with the smart meter, allowing you to monitor your appliances' electricity usage in real time, but your utility company will NOT have the ability to temporarily shut off power to any of these devices.
3. You will have a smart meter installed at your home, and all your appliances will be fitted to communicate with the smart meter, allowing you to monitor your appliances' electricity usage in real time. In addition, your utility company will also have the ability to temporarily shut off power to any of these devices to avoid brownout conditions.

Data Sharing

1. Your data will be collected locally for your personal use and will not be transmitted to the utility company
2. Your data will be transmitted to the utility company for its use but will not be shared with other outside parties. Your utility company will take measures to protect your data, with no guarantees
3. Your data will be transmitted to the utility company for its use and will be shared with the federal government in order to help them better understand energy consumption in the United States. Your utility company will take measures to protect your data, with no guarantees
4. Your data will be transmitted to the utility company for its use and the utility reserves the right to share your data with marketing firms that may give you special offers on products based on your energy consumption. Your utility company will take measures to protect your data, with no guarantees

Example Scenario

In this scenario, please assume that your electric utility company has asked if you would volunteer to participate in a new program. Under this program, you will have a smart meter installed at your home, and all of your appliances will be fitted to communicate with the smart meter, allowing you to monitor your appliances' electricity usage in real time, but your utility company will NOT have the ability to temporarily shut off power to any of these devices. Your data will be transmitted to the utility company for its use and will be shared with the federal government in order to help them better understand energy consumption in the United States. Your utility company will take measures to protect your data, with no guarantees.

Appendix B: Instrument Items

Table B1. Instrument Items

Construct	Original item	Adapted item	Source
IUIPC—control	Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. Consumer control of personal information lies at the heart of consumer privacy. I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	Information privacy is a matter of my right to exercise control and autonomy over decisions about how my electrical usage information is collected, used, and shared. Consumer control of personal electrical usage information lies at the heart of consumer privacy. I believe that information privacy is invaded when control over my electrical usage data is lost or unwillingly reduced as a result of smart meter installation.	Malhotra et al. (2004)
IUIPC—awareness	Companies seeking information online should disclose the way the data are collected, processed, and used. A good consumer online privacy policy should have a clear and conspicuous disclosure. It is very important to me that I am aware and knowledgeable about how my personal information will be used.	Companies collecting electrical usage data should disclose the way the data are collected, processed, and used. Information privacy policies regarding collection of electrical usage data should be disclosed clearly and conspicuously. It is very important to me that I am aware and knowledgeable about how my personal electrical usage information will be used.	Malhotra et al. (2004)
IUIPC—collection	It usually bothers me when online companies ask me for personal information. When online companies ask me for personal information, I sometimes think twice before providing it. It bothers me to give personal information to so many online companies. I'm concerned that online companies are collecting too much personal information about me.	It usually bothers me that my electric company asks me for personal information. When my electric company asks me for personal information, I sometimes think twice before providing it. It bothers me to give personal information to my electric company. I'm concerned that my electric company is collecting too much personal information about me.	Malhotra et al. (2004)
Trusting beliefs	Online companies would be trustworthy in handling (the information). Online companies would tell the truth and fulfill promises related to (the information) provided by me. I trust that online companies would keep my best interests in mind when dealing with (the information). Online companies are in general predictable and consistent regarding the usage of (the information). Online companies are always honest with customers when it comes to using (the information) that I would provide.	My electric company would be trustworthy in handling the data it collects about my electrical usage. My electric company would tell the truth and fulfill promises related to how it uses the electrical usage data it collects from me. I trust that my electric company would keep my best interests in mind when dealing with my electrical usage data. In general, my electric company is predictable and consistent regarding the usage of my personal information. My electric company is always honest with me when it comes disclosing how it uses my electrical usage data.	Jarvenpaa & Tractinsky (1999)

Table B1. Instrument Items

Risk beliefs	In general, it would be risky to give (the information) to online companies. There would be high potential for loss associated with giving (the information) to online firms. There would be too much uncertainty associated with giving (the information) to online firms. Providing online firms with (the information) would involve many unexpected problems. I would feel safe giving (the information) to online companies.	In general, it would be risky to allow my electric company to collect data associated with my electrical usage. If my utility company collected data about my electrical usage, there would be a high potential for that data to be lost or stolen by unauthorized parties. There would be too much uncertainty associated with allowing my electric company to collect data about my electrical usage. Allowing my electric company to collect data about my electrical usage would involve many unexpected problems. I would feel uneasy allowing my electric company to collect data about my electrical usage.	Jarvenpaa & Tractinsky (1999)
Psychological ownership	I sense that this organization is OUR company. I feel a very high degree of personal ownership for this organization. I sense that this is MY company. Most of the people that work for this organization feel as though they own the company.	In my opinion, data collected about my electricity consumption is MY data. I feel a very high degree of personal ownership for my electrical usage data. I think about information related to my personal consumption of electricity as MY information. Most electric consumers feel as though they own their electrical usage data.	Van Dyne & Pierce (2004)
Social influence	People who influence my behavior think that I should use the system. People who are important to me think that I should use the system. The senior management of this business has been helpful in the use of the system. In general, the organization has supported the use of the system.	People who influence my behavior would want me to install smart meters at my home. People who are important to me would believe that installing smart meters is a good idea. People who influence my behavior would be helpful in my use of smart meters. In general, people who are important to me would support the installation of smart meters.	Venkatesh et al. (2003)
Attitude toward SMT	Security measures such as implementing anti-virus software, firewalls, or system updates on your home computer are a good idea. Taking security measures to protect your home computer is important. I like the idea of taking security measures to secure my home computer.	Given these circumstances, installing smart meters at my home would be a good idea. It would be important to install smart meters at my home in this situation. Under these conditions, I like the idea of installing smart meters at my home.	Anderson & Agarwal (2010)
Behavioral intention	I intend to use the system in the next <n> months. I predict I would use the system in the next <n> months. I plan to use the system in the next <n> months.	Given these conditions, it is likely that I would allow smart meters to be installed in my home. In this situation, I predict I would allow the installation of smart meters in my home. Under these circumstances, I would plan on permitting the installation of smart meters in my home.	Venkatesh et al. (2003)

Appendix C: Correlations

Table C1. Correlations

	BI	AB	MI	IUIPC	TPA	PB	OWN	RB	SI	TB
BI	--									
AB	0.255***	--								
MI	-0.178***	-0.045	--							
IUIPC	-0.201***	-0.092*	0.020	--						
TPA	-0.245***	-0.014	0.180***	-0.021	--					
PB	0.063	0.004	-0.001	-0.003	0.020	--				
OWN	-0.109**	-0.071	-0.014	0.634***	-0.064	-0.028	--			
RB	-0.267***	-0.110**	0.040	0.735***	0.007	-0.018	0.615***	--		
SI	0.363***	0.273***	-0.038	-0.180***	-0.040	0.042	-0.217***	-0.185***	--	
TB	0.372***	0.301***	-0.064	-0.311***	-0.020	0.048	-0.174***	-0.387***	0.488***	--

* = p < .05; ** = p < .01; *** = p < .001
BI = behavioral intention, AB = avoiding brownouts, MI = meter invasiveness, IUIPC = Internet users' information privacy concerns, TPA = third party access, PB = program benefits, OWN = psychological ownership, RB = risk belief, SI = social influence, TB = trusting beliefs.

About the Authors

Merrill Warkentin is the James J. Rouse Professor of Information Systems in the College of Business at Mississippi State University. His research, primarily on the impacts of organizational, contextual, and dispositional influences on individual computer user behaviors in the context of information security and privacy and in social media, has appeared in *MIS Quarterly, Journal of MIS, Journal of the AIS, European Journal of Information Systems, Information Systems Journal, Decision Sciences, Information & Management*, and others. He is the author or editor of seven books and has co-authored over 300 published manuscripts, including over 75 journal articles, and Google Scholar reports over 12,000 citations to his work (h-index = 30). He serves or has served in editorial roles for *MISQ, ISR, EJIS, I&M*, *AIS-TRR*, *DSJ*, and other journals. He has held officer and other leadership positions at AIS, DSI, IFIP, and ACM. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and others. He has chaired several international conferences and was the Program Co-Chair for the 2016 AIS Americas Conference on Information Systems (AMCIS) in San Diego.

Sanjay Goel is a Professor and Chair of the Information Security and Digital Forensics Department in the School of Business, Director of Forensics Analytics Complexity Energy Transportation and Security Center, and Director of Research at NYS Center for Information Forensics and Assurance at the University at Albany, SUNY (UAlbany). He received his PhD from Rensselaer Polytechnic Institute and has worked at General Electric Global Research prior to starting at UAlbany. His research interests include information security, cyber warfare, complex systems, security behavior and cyber physical systems He won the promising Inventor's Award in 2005 from the SUNY Research Foundation. He has received, the SUNY Chancellor's Award and UAlbany president's award for Excellence in Teaching, UAlbany Excellence in Research Award, SUNY Chancellor's Award and UAlbany president's award for Excellence in Service, the Graduate Student Organization Award for Faculty Mentoring, and was named an AT&T Industrial Ecology Faculty Fellow. He has received over 8 million dollars in research funding from: NIJ, U.S. DOE, NSF, UTRC, NYSERDA, AT&T, U.S. Department of Commerce, IARPA, AT&T Foundation, James S. McDonnell Foundation, and Blackstone Foundation..

Philip Menard is an Assistant Professor of Information Systems at the University of South Alabama. He received his PhD from the Department of Management and Information Systems at Mississippi State University and is also a past recipient of the US NSF CyberCorps Scholarship for Service (SFS). He is particularly interested in the impacts of security measures on organizational end users, security education training and awareness (SETA) programs, and the impact of espoused cultural values on individuals' performance of secure behaviors. He has published at the *Journal of Management Information Systems*, the *Journal of the Association for Information Systems*, and the *Journal of Computer Information Systems*. He has presented his work at several conferences, including the Americas Conference on Information Systems (AMCIS) and the Hawaii International Conference on Systems Sciences (HICSS). He has served as a reviewer for several IS journals and conferences.