Information Systems Research
Vol. 26, No. 4, December 2015, pp. 639–655
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)

http://dx.doi.org/10.1287/isre.2015.0600

Research Commentary

Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box

Tamara Dinev
Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, Boca Raton, Florida 33431, tdinev@fau.edu

Allen R. McConnell
Department of Psychology, Miami University, Oxford, Ohio 45056, allen.mcconnell@miamioh.edu

H. Jeff Smith
Department of Information Systems and Analytics, Farmer School of Business, Miami University, Oxford, Ohio 45056, jeff.smith@miamioh.edu

Recently, several researchers provided overarching macromodels to explain individuals' privacy-related decision making. These macromodels—and almost all of the published privacy-related information systems (IS) studies to date—rely on a covert assumption: responses to external stimuli result in deliberate analyses, which lead to fully informed privacy-related attitudes and behaviors. The most expansive of these macromodels, labeled "Antecedents–Privacy Concerns–Outcomes" (APCO), reflects this assumption. However, an emerging stream of IS research demonstrates the importance of considering principles from behavioral economics (such as biases and bounded rationality) and psychology (such as the elaboration likelihood model) that also affect privacy decisions. We propose an enhanced APCO model and a set of related propositions that consider both deliberative (high-effort) cognitive responses (the only responses considered in the original APCO model) and low-effort cognitive responses inspired by frameworks and theories in behavioral economics and psychology. These propositions offer explanations of many behaviors that complement those offered by extant IS privacy macromodels and the information privacy literature stream. We discuss the implications for research that follow from this expansion of the existing macromodels.

Keywords: privacy; macromodels; elaboration likelihood model; behavioral economics; psychology
History: Hock Hai Teo, Senior Editor; Corey Angst, Associate Editor. This paper was received on September 9, 2013, and was with the authors 11 months for 3 revisions. Published online in *Articles in Advance* November 20, 2015.

Introduction

Concerns about information privacy have been growing since the 1960s (e.g., Consumers Union 2008, Equifax 1995, Harris Interactive 2011, Sobel 1976, Westin 1967), but the majority of privacy-related research articles addressing these concerns and the related privacy behaviors have been published since the mid-1990s. Recently, some rigorous attempts to provide an overarching model that explains this research stream were undertaken. In the December 2011 issue of *MIS Quarterly*, Smith et al. (2011) introduced a macromodel they called "Antecedents–Privacy Concerns–Outcomes" (APCO), which summarized almost all of the positivist empirical assessments of privacy up to that date. In the same time frame, Li (2011) and Bélanger and Crossler (2011) published similar reviews,[1] and their conclusions were similar to those of Smith et al. (2011) in terms of classifying the variables that have been considered in prior research: antecedents (usually, individual traits or contextual factors) lead to individuals forming privacy concerns, which result in behavioral outcomes based on the individual's information processing. In fact, the construct "concern for information privacy" (CFIP) plays an important role in these three macromodels (Bélanger and Crossler 2011, Li 2011, Smith et al. 2011).[2] Although these authors' macromodels do not fully converge, they capture the empirical privacy-related predictive studies from the past two decades.

The three macromodels share the tacit assumption of the vast majority of the existing information systems

[1] See Pavlou (2011) for an overview of the Bélanger and Crossler (2011) and Smith et al. (2011) reviews.

[2] Hong and Thong (2013) recently provided an in-depth examination of alternatives to measuring Internet privacy concerns, which are related to but in some ways distinct from CFIP. Interested readers are urged to consult Hong and Thong (2013).

(IS) research stream based on economics theory: human beings are capable of making decisions by engaging in effortful, deliberate information processing in forming privacy-related perceptions (Ariely 2009). These articles further assume that this processing is bereft of biased assumptions or cognitive shortcuts.

In fact, however, many individuals engage in privacy-related behaviors spontaneously, often in circumstances (e.g., emotionally charged situations, when one is mentally fatigued) where little deliberation takes place. Accordingly, individuals frequently become the victims of simple heuristic processing and cognitive shortcuts, or they become unduly influenced by extraneous factors (i.e., information that should have no bearing on reasoned decision making). Sometimes behaviors are emotion-laden, spontaneous, or performed without complete information. Prior work on information privacy has rarely accounted for these types of behaviors, and the processes involved in such biased, incomplete decision making and information processing have not been considered.

It has by far been the exception, rather than the norm, for privacy researchers to consider alternative models and explanations outside the APCO model. Studies conducted by Acquisti (2004), Acquisti and Grossklags (2005), Acquisti et al. (2012), Grossklags and Acquisti (2007), Tsai et al. (2011), Li et al. (2008, 2011b, and Xu et al. (2010) were designed to capture contextual or situational effects on privacy behaviors. By employing principles from psychological experiments and behavioral economics, these authors showed that individuals make privacy decisions inconsistently, a finding that is at odds with the APCO model. For example, these experiments demonstrated that people, under diverse circumstances and contexts, may assign different "prices" to privacy: the price to protect a piece of information may differ from the price to sell the same piece of information (Acquisti and Grossklags 2005). Acquisti et al. (2012) showed how the order of intrusive questions can have an effect on disclosure behavior. Li et al. (2008, p. 51) showed that emotions play a large role in how consumers form privacy beliefs and that they take "heuristic shortcuts" to act on those beliefs. These researchers offered some intriguing demonstrations of these important, yet heretofore unexplored and not fully explained, privacy-related phenomena.

There have been calls in business research to revisit and expand the economics principle of rational behavior and to pay close attention to behavioral economics (Ariely 2009, Lee et al. 2009). Furthermore, business practitioners have been advised to pay attention to these same concepts. In a *Harvard Business Review* article, Ariely (2009, p. 78) writes: "Your company has been operating on the premise that people—customers, employees, managers—make logical decisions. It's time to abandon that assumption." He further argues that by adopting a behavioral economics approach, "firms can discover the truth underlying their assumptions about customers, employees, operations, and policies" (Ariely 2009, p. 80).

Just as with business research in general, however, mainstream IS research has paid scant attention to these calls. In a recent editorial in *MIS Quarterly*, Goes (2013, p. iii) recommends incorporating the developments of behavioral economics into the neoclassical economics-driven models in IS research "built on assumptions about rationality of human behavior." This is particularly important for privacy and security behaviors because they are known to be context dependent and demonstrate paradoxical behaviors that are not easily explained by the neoclassical economics models.

We begin our discussion by clarifying some of the nomenclature associated with "high-effort" and "low-effort" cognitive processing. Next, to illustrate the limitations associated with the mainstream APCO approach, we provide an example of an individual facing a privacy-related behavioral decision and then explain the person's behavior by peering through two lenses: (1) the mainstream, original APCO model and (2) an enhanced APCO model that includes consideration of lower-effort cognitive processes and biases in human decision making. We advance propositions that serve to inform privacy research and identify significant yet unexplored aspects of privacy-related behaviors that demonstrate the importance of two domains: (a) when affect (i.e., emotions, mood) or cognitively depleting conditions are present in formulating privacy-related behavioral responses and (b) when well-known cognitive biases and extraneous factors such as framing, anchoring, loss aversion, and others influence beliefs and behaviors. We conclude by offering a set of recommendations for enhancing the privacy research stream.

Levels of Effort Nomenclature

Throughout this commentary, we refer to "high-effort" and "low-effort" cognitive processing. These terms have their origin in the heuristic-systematic model (Chaiken 1978, 1980) and in the elaboration likelihood model (ELM; Petty and Wegener 1998). Both models distinguish—in quite a similar manner—more effortful from less effortful information processing and decision making. On a few occasions, some IS researchers have considered the ELM in studies related to information privacy. For example, Angst and Agarwal (2009) used the ELM to show that attitudes regarding e-health records are directly affected by message framing, and that this direct effect is moderated by the level of privacy concern. Additionally, Bansal et al. (2008) showed that context and privacy concerns have moderating

roles in building trust for privacy assurance mechanisms. Also, Lowry et al. (2012) used the ELM to show that privacy assurance is most effective when seals and statements are accompanied by the peripheral cues of website quality and brand image. Although these studies made good use of the ELM, they were not expressively concerned with subjects' processing approaches (low effort or high effort).

The ELM proposes that there are two processing "routes" by which attitudes are formed and behaviors enacted: the central route and the peripheral route. When following the central route, it is assumed that people form, change, and act on their attitudes through a high-effort process that is elaborated, consciously determined, logical, and explainable. By contrast, the peripheral route involves relatively little cognitive effort or conscious awareness, reflecting low-effort cognitive processing (Petty and Cacioppo 1981).

Furthermore, when explaining behaviors associated with low cognitive effort, some behavioral economics researchers use the term "irrational" (see, for example, Ariely 2008, 2009). We prefer to follow the psychological research nomenclature that avoids using terms such as "irrational," "nonrational," and "nonconscious" because they are difficult to define and do not characterize underlying cognitive processes. Additionally, modern psychological theories focus on a continuum ranging from high-effort to low-effort processing of stimuli, avoiding the binary treatment resulting from "rational–irrational" terminology (Petty and Wegener 1998).

Whether one subscribes to ELM or similar variants of modeling behavior, the key themes are the same. Specifically, decision making can involve greater amounts of deliberation and mental effort (high-effort processing) or involve relatively little mental effort, resulting in a relatively greater reliance on automatic heuristics (low-effort processing). Thus, we focus on high-effort and low-effort processes in the current work, highlighting how privacy stream researchers might benefit from a greater appreciation of low-effort processes and their role in determining privacy-related behaviors.

With these nomenclature clarifications, we now turn to an example of an individual who employs low-effort processing when making a privacy-related decision.

An Example of Low-Effort Processing in a Privacy-Related Decision

Gladys is a well-adjusted professional person who usually makes very deliberate decisions. She has no known personality disorders or addictions. She guards her privacy and very selectively discloses private information about herself, limiting such disclosure to her core needs such as banking, online shopping from well-established websites, and engaging with trusted hospital information portals. She does have a small collection of high-end purses, and she enjoys looking at extremely expensive ones—even those in the $50,000 price range—although she would never consider purchasing an item with such a price tag.

One day, after several intense hours at the office, Gladys discovered the website of a firm based in another country that offered what appeared to be well-constructed versions of the purses she desires—but at prices less than $1,000 each! Gladys was so enthralled by this offer—and by the apparent quality of the purchases she saw on the firm's website—that she responded to an offer to become a "Diamond-level" member with access to a special collection of limited edition purses. The only requirement for this "Diamond-level" membership was that Gladys provide her email address and a few pieces of personal information (her name, address, and information about her previous purchases and other apparel). Gladys was well aware of the potential for abuse of the information, but she nevertheless entered the information so as to gain access to the special purse collection. The next day, she felt great regret regarding her action—and she was even more chagrined a few days later when she began to receive email spam that seemed to have resulted from her action.

Although this example describes a woman, the phenomenon is frequently observed across both genders. Individuals who encounter online opportunities associated with their own hobbies or passions—such as rare vintage or international music or movies, performances, stamp or coin collections, fishing gear, collectible sports items, exclusive offers for sporting events, luxurious car accessories, etc.—may succumb to this approach to decision making.

In what follows, we first consider the original APCO model, which relies on high-effort cognitive processing, and we demonstrate how a researcher who embraces it will encounter difficulties in explaining Gladys's behavior. We will then show how an enhanced APCO model, which incorporates low-effort processing and biases, provides a more complete account of Gladys's behavior.

The Original APCO Model

By considering the aforementioned macromodels (Bélanger and Crossler 2011, Li 2011, Smith et al. 2011), we can conclude that (1) various factors influence privacy concerns at several levels, (2) a number of factors mediate and moderate relationships between privacy concerns and intentions and behavior, and (3) there are many privacy-related intentions and behaviors (e.g., disclosures) that can be observed at many different levels (especially individual and societal). More important, all three of these macromodels share a critical assumption that *responses to external stimuli result in deliberate analyses, which lead to fully informed privacy-related attitudes*

and behaviors. Each of these macromodels assumes that individuals reflect thoughtfully and deliberately on their behaviors involving privacy options; however, none of these macromodels considers the nontrivial impact of low-effort thinking and extraneous influence of default heuristic processes and biases when a decision is made. In other words, features of the decision making context (and not factors involving personality traits, demographics, or decision-making antecedents) can lead to suboptimal privacy-related behaviors because decision makers rely on cues and automatic responses that are unrelated to relevant information that presumably underlies reasoned, thoughtful action. Thus, important considerations, such as one's emotional state or cognitive biases (Goes 2013), are overlooked by these macromodels. This weakness is not merely a deficiency of the models, per se, but of extant IS privacy research because all three models are built on the literature they review.

Because it purports to explain the widest domain of behaviors and to consider the most exhaustive set of inputs, we focus our attention on the APCO macromodel (Smith et al. 2011). Without explicitly acknowledging it, the APCO model assumes that people are engaged in high-effort, thoughtful processing of information and stimuli.

To explain Gladys's behavior through the original APCO model, one would follow this logic: Gladys would have compared the benefits she would receive from providing her information (purchasing a fabulous bag at an incredible discount) to the costs and risks of disclosing information to an unknown vendor (e.g., time to deal with potential spam, possible sale of her information to other firms, possible misuse of her personal identity for financial or other fraud). Gladys would have calculated the positive utility from this benefit and subtracted the negative utility (which would have required some estimation of both the size of the costs as well as the stochastic probabilities of each risk, likely normalized by Gladys's privacy concerns, which would be derived from other factors), leaving her with either a net positive or a net negative sum. Based on the sign of this sum, Gladys would have decided whether or not to provide the information.

To the extent that Gladys's analysis led to a dysfunctional outcome, a rationalist (e.g., Simpson et al. 2002) would likely explain this by the fact that Gladys lacked full information about the use and misuse of any data she might provide. If pressed, the rationalist might concede that some of the antecedent factors in the APCO model—particularly those associated with personality traits such as need for immediate gratification and low self-control (see Pratt and Cullen 2000) and paranoia—could also have impacted her level of privacy concern, which could then have played a small role in the normalization described above. Based on the APCO model, this is the only context in which any of Gladys's personal factors would be taken into account; beyond that, the rationalist would contend that all decision makers would reach the same conclusion as Gladys given the same situation and set of facts. Additionally, the rationalist would ignore any time or emotional pressures that may have led Gladys to render faulty estimates of costs, benefits, or stochastic probabilities.

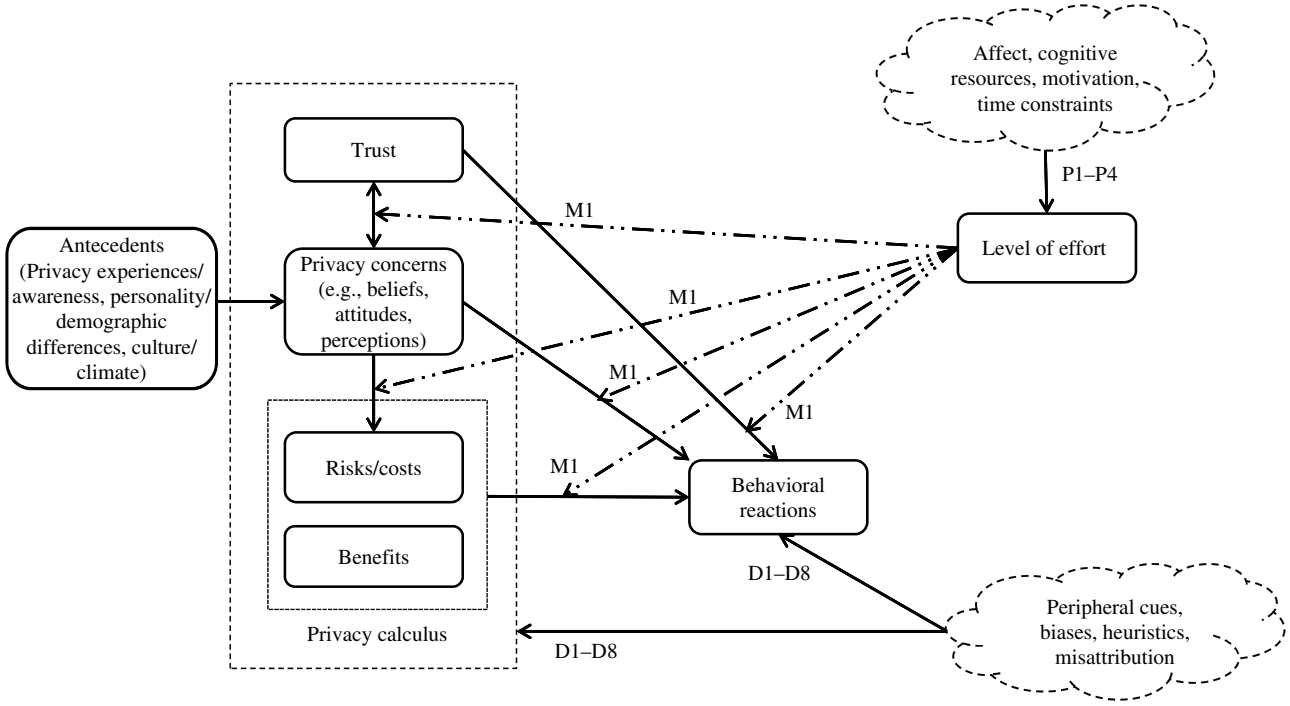
Although the rationalist's interpretation of Gladys's decision making would be consistent with the modeling of privacy-related behaviors found in much of the IS literature, we claim that it provides an incomplete explanation for two reasons. First, recall that Gladys regretted her decision by the following day even though she did not have any additional information at that point. Because nothing would have changed in her cost–benefit analysis during those 24 hours, from a rationalist's view, Gladys's analysis should have remained consistent over this time period. Second, it is undeniable that Gladys's feelings of excitement clouded her judgment. Her behavior was characterized by a limited or bounded rationality (what is reflected in colloquial terms such as "clouded" or "hastened" judgment) in her cost–benefit analysis. Gladys's heightened emotional state led her down a low-effort processing path; however, such a course is not incorporated in the privacy macromodels described above. Nonetheless, important advances in the psychology and behavioral economics literatures identify that low-effort, more automatic processes are powerful determinants of behavior (e.g., Briñol and Petty 2012, McConnell and Rydell 2014, Petty and Wegener 1998). In the next section, we demonstrate that macromodels of privacy research (Bélanger and Crossler 2011, Li 2011, Smith et al. 2011) would benefit considerably from incorporating low-effort processing and extraneous factors that influence judgment and decision making into their accounts of privacy-related behaviors.

The Enhanced APCO Model

We now offer a more comprehensive explanation of privacy-related behaviors (such as Gladys's) that incorporates important elements ignored by past theories, including the level of cognitive effort being expended by an individual, several factors that impact that level of effort,[3] and extraneous influences (e.g., peripheral cues, biases) that may affect constructs within the APCO macromodel. Figure 1 presents these important additions to APCO, adding two "clouds" that influence

[3] The level of cognitive effort being expended is determined by a number of complex factors, including motivation to process, self-relevancy, ability to process, and many others. A detailed examination of this full model is beyond the scope of this commentary. See Petty and Cacioppo (1981, 1986) for details.

Figure 1 Enhanced APCO Model



privacy-related attitudes and behaviors. The upper "cloud" represents a set of situational and cognitive limitations that determines the level of effort of processing (the effects shown with arrows and denoted by P1–P4 on Figure 1). We propose that level of effort modifies the original APCO relationships (this effect shown with dashed lines and denoted by M1), and we elaborate on these implications below. The lower "cloud" represents important extraneous influences that have been identified by the fields of behavioral economics and psychology: biases, heuristics, and misattributions that directly influence privacy-related attitudes and behaviors without much intention, awareness, or cognitive effort (shown with arrows and denoted by D1–D8). These biases, heuristics, and misattributions are always present in one form or another, and they are distinct from antecedent factors related to the individual (e.g., personality traits, demographic differences) or climate (e.g., cultural influences, commonly held stereotypes) because they are features of the decision making context itself that guide privacy behaviors in ways that, from an objective perspective, should have no bearing on the actions undertaken. When an individual is engaged in high-level processing, the influence of these extraneous effects is muted by the relationships that are grounded in deliberate analysis (those in the original APCO model). As processing effort moves from high to low, the impact of extraneous influences becomes greater, possibly to the point that they dominate decision making.

The psychology and behavioral economics literature streams enumerate and examine a multitude of situational and cognitive limitations and biases. Without attempting to document an exhaustive list, we include those that are studied frequently and that have been researched and confirmed by multiple research teams. What follows is a more detailed description of the two "clouds," the level of effort, and the direct and indirect effects on APCO. We derive important new propositions based on this enhanced model.

Level of Effort and the APCO Relationships

As noted earlier, almost all of the past studies undertaken within the IS research stream have assumed high-effort processing, which epitomizes the behavioral paradigm of neoclassical economics. The original APCO model, as a reflection of extant IS research, assumes that privacy-related behaviors are enacted through deliberate, high-effort processes as well.

By contrast, low-effort processing involves relatively little cognitive effort or conscious awareness; that is, behavior-relevant information is evaluated by means of simple and relatively automatic cognitive heuristics and mental shortcuts that are based on past experiences, habits, routines, inertia (Polites and Karahanna 2012, 2013), or spontaneous reactions rather than on effortful analysis involving logic and elaborated reasoning. These mental shortcuts can result in suboptimal behaviors that run contrary to one's expressed beliefs and values, and conditions can be crafted that take advantage of these pitfalls in judgment and decision making (e.g., Ariely 2008, Cialdini 2009, Lehrer 2009).

The level of effort framework easily explains privacy-related behaviors that are difficult to reconcile with the original APCO model, especially behaviors that run contrary to one's beliefs, values, or historical and future behaviors under the same circumstances. In colloquial language, phrases such as "clouded judgment," "hasty decision," "what was I thinking?," "misguided decision," "impulsive act," and "don't think twice" all refer to cases when deliberate, full, thoughtful processing of all information and stimuli is absent or low-effort shortcuts have been followed.

From the "level of effort" lens comes two important implications for privacy research models: (1) Depending on the circumstances, privacy-related decisions can be enacted along a continuum ranging from low effort to high effort. As a result, any research macromodel that considers only deliberate, effortful processes and ignores low-effort processes will be incomplete. (2) Attitudes that are changed and behaviors that are enacted by low-effort processing are generally weaker and shorter lived than the attitudes and behaviors produced by high-effort processing. Low-effort processing involves influences of transient factors that are often unrelated to the privacy decisions at hand (e.g., emotions, mood, time constraints, cognitive depletion), yet, as will be explained later, they can influence actions significantly.

In the enhanced APCO model, the level of effort determines the extent to which original APCO relations are weaker or stronger. If high-effort processing is present, privacy-relevant information will be processed deliberately and logically, consistent with the tenets of the original APCO model. However, if low-effort processing is present, some relationships within the original APCO model may be impacted, although the specific directionality of those impacts can depend on numerous factors. For example, consider the division of people into the categories of "privacy fundamentalists," "privacy pragmatists," and "privacy unconcerned" (Equifax 1995, p. 13). Under low-effort processing, the relationships can be expected to *weaken* for privacy pragmatists, suggesting a lesser inclination to engage in effortful activities that might preserve one's privacy (e.g., thoroughly scrutinizing a "terms of service" agreement or analyzing the consequences of disclosure). However, some of the relationships in the APCO model may be *strengthened* for a privacy fundamentalist: for example, the relationship between privacy concerns and risk might strengthen under conditions of low-effort processing (similarly, that same relationship might weaken under low-effort processing for a privacy unconcerned individual). Because the specific moderating effect (strengthening or weakening) cannot be predicted in absolute terms a priori for each relationship, further empirical research will be needed to address the exact ways in which level of effort modifies the APCO relationships. In fact, there may be a need for special methods that treat complex moderated-mediation effects as well as pure moderation or pure mediation effects (Preacher et al. 2007).

Proposition M1. *The level of effort employed in processing information regarding privacy-related decisions moderates the APCO relationships in forming privacy-related attitudes and behaviors*.

Of great importance are the factors that determine the level of effort used by an individual in making privacy decisions, and we now discuss these factors.

Cognitive Resources and Affect as Drivers of Level of Effort

Several factors have been shown to undercut high-effort processing, including affect (emotions and mood), time constraints, limited cognitive resources, and the need for cognition (Cacioppo and Petty 1982, Kahneman et al. 1982, Schwarz and Clore 2007). All of these factors, alone or in combination, can move people away from high-effort processing and toward low-effort information processing. Below we consider these factors in more detail and develop relevant propositions.

Information Overload and Limited Cognitive Resources. Following intense cognitive activity, people have fewer attentional resources to engage in information elaboration, resulting in more low-effort processing and greater influence of heuristic and cognitive biases (Petty and Wegener 1998, Shiv and Fedorikhin 1999, Shiv et al. 2005). When people are cognitively depleted (e.g., tired, at the low-end of their circadian cycle), they are more likely to take cognitive shortcuts rather than study, scrutinize, and evaluate privacy-related information. To the extent that "easy actions" entail greater privacy risks, cognitive depletion could put people's privacy at risk. Returning to our example involving Gladys, it is easy to imagine that her being exhausted at the end of a hard day increased the likelihood of her engaging in low-effort processing (e.g., "saving money is attractive") rather than effortful scrutiny of the website she encountered (e.g., "I should be wary of foreign websites from nonestablished companies"). A person in a similar mental state might react in the same manner when confronted with a brand new website offering rare music not available on Amazon or iTunes. Or, after a long and tiresome day, a person might post a controversial message or picture on Facebook or Twitter that leads to later regrets for that post.

Proposition P1. *People with reduced cognitive resources or who are cognitively taxed will be more likely to engage in low-effort processing*.

Affect: Implications of Emotion and Mood. As noted by Zhang (2013), important strides in understanding IS-related phenomena result from researchers incorporating affect into their models. Ironically, however, the privacy research stream includes very few studies that consider the role of affect (Li et al. 2008, 2011b are rare exceptions). It seems that often emotions are high and affect is intense in many situations where poor judgment is exhibited in Internet privacy-related behaviors. For example, people in the privacy unconcerned/pragmatist categories may share their electronic contact lists with mobile apps to meet new people when they feel lonely, or disclose credit card information to "verify their age" when their interest in pornography is piqued. When such individuals do not feel socially isolated or sexually aroused, they would be unlikely to divulge information that could lead to their friends and work colleagues being targeted by marketers or risk their own credit credentials to an unknown purveyor of pornography whose URL is from a foreign land. In a converse condition, a privacy fundamentalist might delete her online profiles or cancel online services when in such a state, because she may overreact to innocent information requests from an online provider.

Zhang's (2013) framework and research in the psychology literature speak to the role of affect in determining behavior (e.g., Schwarz and Clore 2007), illustrating the importance of incorporating the role of affect (e.g., emotions, mood) in privacy research. Additionally, the work of Ariely and Loewenstein (2006) and Loewenstein (1996) on visceral influences advances our understanding of affect's role in one's behavior. Their findings indicate that it would be very difficult to explain affect within the framework of a high-effort economic model. Zhang (2013) mentions that affect is an umbrella term that defines a set of basic affective concepts including emotions and mood. *Emotions* are characterized as affective states with sharp rise time, limited duration, and high intensity, and they have a perceived cause (Schwarz and Clore 2007). *Moods*, on the other hand, are affective states that develop more gradually, last for a relatively greater period of time while being lower in intensity, and they do not have a clear referent or cause. For example, one is angry *at someone*, not "just angry." On the other hand, being in a "bad mood" reflects a broad and diffuse state.

When it comes to affect and information processing, typically more intense emotional states (e.g., happiness, physical arousal, fear, anger) reduce one's cognitive resources, making low-effort processing more likely. For example, people experiencing anger (i.e., an intense negative emotion) are more likely to render judgments about others based on stereotypes instead of individuating information (i.e., taking into effortful account a person's unique qualities) because the intensity of their emotional experience reduces processing of detail-relevant information (Bodenhausen et al. 2001), and they are more likely to make poorer decisions in cognitive demanding situations (Gneezy and Imas 2014). Other emotional states, such as guilt, may lead people to engage in more prosocial behaviors to reduce their compunction (Gneezy et al. 2014). On the other hand, intense positive emotions (e.g., elation, physical arousal) also reduce cognitive expenditures, making it more likely that people will rely on shortcuts such as heuristics and stereotypes (Ariely and Loewenstein 2006, Loewenstein 1996) than on more effortful processes (e.g., deliberation, individuation). Thus, when people experience intense emotions, they have fewer cognitive resources available regardless of the valence of their feelings, and as a result, they more likely engage in low-effort rather than high-effort processing.

Research on moods and on diffuse positive or negative feelings without a clear referent reveals more complex consequences for judgment and decision making. For example, research in social and cognitive psychology demonstrates that *happy* moods lead to less effortful processing (e.g., greater reliance on heuristics, stereotypes, expectancies), whereas *sad* moods lead to more effortful processing (Bodenhausen et al. 2001, Schwarz and Clore 2007). In Schwarz and Clore's (2007) mood as information framework, positive mood is interpreted as a signal that "things are okay," and thus one can move ahead without effortfully examining one's environment or behavior. On the other hand, negative mood is interpreted as a signal that "something must be wrong," which leads one to deploy additional attention resources in the service of scrutinizing one's situation to identify better solutions. In short, positive moods are more likely to lead one to engage in low-effort processing, whereas negative moods are more likely to lead one to engage in high-effort processing.

In some cases, if people experience strong emotions along with or after demanding cognitive tasks, the impact of the low-effort heuristics will be even more pronounced. Returning to our earlier example, the intense excitement and joy that Gladys felt when she discovered a website selling what seemed to be high-quality purses at a substantially reduced price made it less likely that she would engage in a thoughtful analysis of the consequences of volunteering her email address and personal data to the website. Instead, she employed low-effort processing that resulted in privacy-risky behavior. On the following day, absent the emotions, she was able to process the same information and stimuli through the high-effort mode that resulted in her regrets. Similarly, people who are excited during a vacation might post Facebook pictures and vivid descriptions about their adventures online, and in the process carelessly reveal private or compromising information about their friends. Later, on learning that

friends were upset, they might reread their posts after their in-the-moment emotions have dissipated and question their impulsive online disclosures.

Proposition P2. *Current intense emotions and moods can impact the level of effort associated with cognitive processing.*

Time Constraints and Need for Cognition. Often, even when individuals have enough cognitive resources to engage in effortful information processing, they may be limited by time constraints. When time is short and a decision needs to be made quickly, people may not engage in a thoughtful, deliberate analysis of the situation regarding privacy-related behavior. In such cases, it is likely that low-effort processes will be invoked instead. Another effect of time constraints is that they may cause anxiety, which in turn depletes the cognitive resources and (as in P1) drives the individual toward low-effort processing. Examples of time constraints concerning information privacy and submitting personal information can include those when a person searches urgently for information regarding a medical emergency or responds to "Act Now!" messages with offers expiring soon.

Proposition P3. *Time constraints can invoke low-effort processing.*

Cacioppo and Petty (1982) identified and measured the construct *need for cognition*, a personality trait that indicates the extent to which individuals are inclined toward effortful cognitive activities. People who have a high need for cognition are more likely to form their attitudes by paying close attention to relevant arguments, and accordingly, they invest more cognitive effort and exhibit more thoughtful processing of information. People who are lower in need for cognition, on the other hand, tend to dislike thinking, and as a result, they reveal more low-effort processing. For example, a study conducted by Cacioppo et al. (1986) found that the attitudes of those high in need for cognition were more predictive of behavioral intentions and reported voting behavior than were the attitudes of those low in need for cognition. All other factors being equal, people with a greater need for cognition can be expected to study online privacy policies in more detail, to question organizations' gathering of personal data, and to consider the involvement of third parties in data sharing.

Proposition P4. *A higher need for cognition invokes high-effort processing, whereas a lower need for cognition invokes low-effort processing.*

Individuals engaged in low-effort processing are more likely to make privacy-related decisions based, at least in part, on factors that fall outside of the original APCO model. Several of those factors are the focus of the next section.

Extraneous Influences: Peripheral Cues, Biases, Heuristics, and Misattribution Effects

To the extent that relationships in the original APCO model are moderated by low-effort processing, other factors (which, as noted earlier, we term "extraneous influences") inherent in the situation unrelated to decision-making quality may influence individuals' privacy-related perceptions and behaviors. Peripheral cues, biases, heuristics, and misattributions have been studied by researchers in psychology and behavioral economics, and they are examples of extraneous influences that may affect some or all of the constructs in the original APCO model.

Individuals are frequently influenced by peripheral cues, biases, heuristics, and misattribution effects, but existing models of privacy-related behaviors have paid little attention to them. Although some scholars such as Goes (2013) have stressed the need to incorporate these categories in our behavioral models, most researchers have not. In this section, we discuss some of the ways in which these extraneous influences can inform privacy research theory. Also, it is important to note that these effects are often combined or intertwined with each other (e.g., one often cannot separate message framing from loss aversion). Thus, privacy-related behaviors may result from the impact of multiple extraneous influences, suggesting that a single study may be unable to conclusively test or evaluate all of the propositions we describe below.

The extraneous influences listed in this section and presented in Figure 1 as the lower "cloud" impact attitudes and behaviors directly (the *D* lines in Figure 1). These direct relationships are automatic in nature and in general cannot be made stronger or weaker. However, it is the level of effort of information processing that will determine their *relative* influence on attitudes and behaviors, that is, whether they will be predominant or overridden. When one engages in deliberate, high-effort level processing, the relative impact of these extraneous influences on attitudes and behaviors is low and negligible. However, under low-effort processing, the relative strength of these extraneous influences on attitudes and behavior will increase. In other words, rather than employ logic and reasoning in forming privacy-related attitudes and behavior, people who exhibit low-effort processing will be more influenced by a variety of extraneous influences including cognitive biases, perceptual distortions, inaccurate judgments, and greater reliance on stereotypes, and overly simplistic rules of thumb (Ariely 2008, Bodenhausen et al. 2001, Cialdini 2009, Kahneman et al. 1982).

We now discuss the peripheral cues, biases, heuristics, and misattribution effects in more detail. In each section, we discuss the most likely associations with certain APCO constructs. As we will explain in each section,

the exact nature of the impact is contextual, depending on how the extraneous influences are expressed or used. Thus, for illustrative purposes, in Figure 1 we denote the derived propositions D1–D8 with two arrows from the lower cloud. We use the phrase "APCO model constructs" in the propositions to indicate that one or more APCO constructs may be impacted by each of the extraneous influences examined below.

Peripheral Cue: Message Framing. Inspired largely by the groundbreaking research of Tversky and Kahneman (1981), behavioral economists have long accepted that people react differently to a message depending on whether it is framed as a loss or as a gain (Goes 2013). One of Tversky and Kahneman's (1981) most famous examples is that of physicians whose treatment decisions varied greatly depending on whether the rates of effectiveness for treatment options were framed positively (in terms of how many lives will be saved, which led to 73% of physicians picking a certain treatment) versus negatively (in terms of how many lives will be lost, which led to 22% of physicians picking that same treatment).

Message framing should impact decision making more strongly under low-effort conditions (Cacioppo et al. 1986, Cialdini 2009, Petty and Wegener 1998, Smith and Levin 1996). Accordingly, framing effects are typically observed more for people who engage in low-effort processing such as for those who are lower in need for cognition (for a review, see Petty and Wegener 1998), though there are times when other factors such as valence qualify this general phenomenon (Levin et al. 1998, Zhang and Buda 1999). Some IS studies have examined the impact of message framing on privacy and on trust: Angst and Agarwal (2009) showed that greater concerns for privacy can be alleviated by appropriate message framing, and Lowry et al. (2012) showed that privacy assurance is most effective when seals and statements are accompanied by the peripheral cues of website quality and brand image. In the context of privacy- and security-related behaviors, of particular importance are the fears of immediate threat invoked in some messages (see, for example, emotion-focused coping in Liang and Xue 2009). Several studies have shown that fear and threat of immediate danger or loss affect individuals' perceptions (e.g., Baron et al. 1992, Rogers 1983). A message framed as an immediate danger or threat can directly impact both risk and behavioral reactions.

It is important to distinguish between fear appeals in messages aimed to discourage a planned illegal or risky behavior (e.g., warning of consequences of criminal behavior, smoking, piracy, illegal downloading, security breaches; see Johnston and Warkentin 2010) and those that invoke fear of immediate threat or loss. The former fear appeals refer to a more thoughtful and deliberate decision-making cost–benefit analysis because the behavior is not immediate, but instead is a result of a well-planned and thoughtful process. By contrast, fears of immediate loss and threat are known to invoke immediate reaction, particularly because time and cognitive resources cannot be devoted to more thoughtful processing. For example, threatened by a loss of their data in their computer, individuals may click a link to download "scareware," a type of malware that presents itself as antivirus software and relies on frightening messages such as "Your computer is infected, you risk losing your data and your identity" to lure users. Similar tactics are employed by threatening spoof emails as if from the Internal Revenue Service ("your tax filing is overdue . . . click here to reinstate your account") or professional licensing authorities ("your CPA certification will be revoked if you do not click here and verify your certification").

Depending on how a message is framed (e.g., negative versus positive, trust versus privacy, risks versus benefits), one or more APCO constructs may be impacted. Above, we described how privacy concerns, risk, and behavioral reactions can be influenced by message framing. Likewise, other APCO constructs can be influenced by this important peripheral cue.

Proposition D1. *Message framing acts as a peripheral cue and can impact the APCO model constructs.*

Endowment and Related Biases. The above concept of framing is related to the set of biases discussed in this section, namely, the *endowment effect*, *loss aversion*, and *zero-cost* biases. Contrary to the principles of classical economic theory, numerous studies have shown that people place a greater value on an object they already own than on the same object when given an opportunity to purchase it, which is known as the endowment effect (Kahneman et al. 1991). Similarly, people have a stronger preference to avoid losses than to acquire gains (and unlike the endowment effect, this is independent of ownership), which is referred to as loss aversion (Tversky and Kahneman 1981, 1991). In short, when it comes to decision making, individuals place a greater value on the things they already possess, and they would rather avoid a loss than make a gain of equal value (Ariely et al. 2005; Kahneman et al. 1991; Tversky and Kahneman 1981, 1991). For example, consumers who were given a coffee mug demanded twice as much to sell it than others were willing to pay to own it because once endowed with it, selling it was perceived as a loss (Novemsky and Kahneman 2005).

An example of how the endowment effect impacts privacy-related behaviors was provided by Acquisti and Grossklags (2005), who showed that the price to protect a piece of information may be different from the price to sell the same piece of information. Thus, all things being equal, individuals engaging in privacy calculus will weigh losses more heavily than gains

when they assess the alternatives. When people see that disclosing personal information or preferences may lead to well-defined "savings" or prevention of financial losses, they will be more prone to disclose such information than when the benefits are framed as "gains," such as "we will be able to serve you better" or "we will give you $ if you register with us."

A derivative of the loss aversion bias is the *zero-cost* bias: providing a "free" alternative (versus one of low cost) has a disproportionately large impact on subjects' assessments (Ariely 2008, Kahneman and Tversky 1979). For example, in one experiment, more people chose a free $10 Amazon certificate than a $20 certificate offered for seven dollars (Shampanier et al. 2007). Because people overreact to the losses and "free" offers, when people are asked about personal information or about being tracked, any reward that appears as a free gift will have a disproportionally large impact on decision making. Thus, in a privacy-related context, an individual might be especially likely to disclose personal data when offered a "free" product or service in return for the data. In addition to the examples above (related to privacy concerns and behavioral reactions), it is easy to see how, depending on the exact context, an offer or message can be framed to directly impact the trust, risk, or benefit constructs in the APCO model.

Proposition D2. *The endowment effect, loss aversion, and zero-cost bias can impact the APCO model constructs.*

Implicit Trust and Positivity Biases. Since the mid-1990s, IS researchers have considered the importance of trust in many contexts, most frequently e-commerce (e.g., Fang et al. 2014, Gefen and Pavlou 2012, Liu and Goodhue 2012, Ou et al. 2014, Özpolat et al. 2013, Rice 2012, Riedl et al. 2010), but also in other contexts such as e-government services (e.g., Lim et al. 2012), interorganizational data exchanges (e.g., Nicolaou and McKnight 2006), online collaboration (e.g., Jarvenpaa and Majchrzak 2010), outsourcing (e.g., Gefen et al. 2008, Rustagi et al. 2008), and virtual teams (e.g., Dennis et al. 2012, Jarvenpaa et al. 2004, Piccoli and Ives 2003). Of immediate interest is that trust has appeared as an important construct in numerous privacy studies (e.g., Bansal et al. 2008, Dinev and Hart 2006, Eastlick et al. 2006, Metzger 2004, Schoenbachler and Gordon 2002, Xu et al. 2005; see synthesis in Smith et al. 2011). What has generally been unconsidered in these studies—not only those associated with privacy but also those in the other IS domains—is that the trust construct may be impacted by at least two different forms of biases:

(1) *Default* (*implicit*) *trust bias*. In the absence of contrary information or argument, people assume that others are honest and cooperative and that what they say is true (Gilbert 1991, Grice 1975, Petty and Wegener 1998, Strack and Schwarz 1992). From infancy, "default trust" bias is established because children are entirely dependent on other people and have little choice but to trust those around them. Additionally, evidence suggesting that normally what people say is true accumulates from infancy, leading to a well-formed bias to trust people's testimony (Jaswal et al. 2010). By employing default trust later in life, we are less inclined to evaluate others' trustworthiness (Möllering 2006). Thus, this trust state reflects a default heuristic rather than a deliberate or conscious choice (Jaswal et al. 2010). For example, most individuals tend to believe companies when they announce that "we do not share your personal data," and for that reason they do not scrutinize detailed company policies to check for vague wording or onerous opt-out policies. Unless people are aware of trust having been comprised, they tend to trust what companies say about using personal data.

(2) *Positivity bias*. Positivity bias (Sears 1983, Stoutenborough 2008) refers to the fact that people tend to evaluate individuals positively and favorably, even in the case of negative evaluations of the group or entity to whom that individual belongs. For example, people typically report hating Congress, but liking their particular congressional representative (Newport 2001, Sears 1983), and they report negative attitudes toward education or healthcare, but report great affinity for their own personal professor or doctor (Hoorens and Buunk 1993, Sears 1983). Similarly, one can expect positivity bias to impact privacy concerns. Consider, for example, that a person might, on one hand, claim that "Internet companies do not care about my privacy, and I hate to disclose information" but, at the same time, frequently disclose information on Facebook and Twitter.

Proposition D3. *Default trust and positivity bias can impact the APCO model constructs.*

Optimistic Bias and "Yes" Bias. The *optimistic bias* and the *"yes" bias* will influence privacy-related behaviors because they will result in underestimations of risk and excessively compliant responses to information requests, respectively. According to the *optimistic bias*, people make overly optimistic estimates regarding a large number of factors, including the probability of "winning" and the calculation of risk (Sharot 2011, Taylor and Brown 1988). For example, consider the underestimation of risk that is revealed by many college students' posting of uncensored pictures and comments on Facebook. Many of these students—who are tagged in photographs showing them in compromised positions and who post comments heralding their overconsumption of alcohol—underestimate the risk associated with such postings falling into the hands of prospective employers, or even their own parents. Another example of underestimated risk—"it won't

happen to me"—is the reckless behavior of politicians and powerful persons. Situations in the public domain often leave observers perplexed as to how individuals in power could be so reckless as to post compromising pictures, send messages on their social network accounts, or use their cell phones or online accounts for illegal activities. In such cases, these individuals underestimated the riskiness of their behavior, and it is clear that these individuals were certainly engaging in low-effort information processing (e.g., in intense emotional states).

The *"yes" bias* refers to the tendency of people to say yes to someone's request and to greatly underestimate the likelihood that they will comply to that request (Flynn and Lake 2008). For example, canvassers are often sent into residential neighborhoods to build support for nonprofit causes such as "green" initiatives. Frequently carrying clipboards and literature, these canvassers ring doorbells and ask for information and support from homeowners. When queried about their responses to canvassers, many homeowners will claim that they do not provide information to those who ask, but in reality the canvassers frequently receive informative responses to at least the first few of their questions before homeowners eventually cease answering and query "what did you say this information is for?" Another frequent behavior that can be explained by the "yes" bias is the readiness with which people give their phone number or email to cashiers at retail stores without even being offered discount cards or coupons.

The influences of the optimistic and "yes" biases will most likely be observed directly in behavioral reactions. However, it is conceivable that these biases could also influence some of the other APCO constructs such as trust.

Proposition D4. *The optimistic and "yes" biases can impact the APCO model constructs.*

Source Variables. Source variables include message-unrelated factors involving the source of a solicitation, such as perceived expertise, attractiveness, likability, power and authority, and other characteristics of the communicator (Cialdini 2009, Petty and Cacioppo 1981, Petty and Wegener 1998). For example, Priester and Petty (1995) found that people often simply accept a message from a source without scrutinizing the source's motives or intents. In everyday life, many customers freely provide their telephone number or email address to retailers, and they are unlikely to question the reason for the request or the use of the information. These customers are probably attributing message-unrelated characteristics such as authority to the cashier, even though the cashier or the store could conceivably misuse the phone number for nefarious purposes. The "yes" bias (see above) could also be an explanation; only a rigorous experiment can identify the underlying cause of these behaviors.

Many source cues can impact one or more of the APCO constructs—trust, risks, benefits, privacy concerns, or behavioral reactions. For instance, one of the social engineering mechanisms that is often exploited for security attacks is taking advantage of the perceived trustworthiness ascribed to people in uniform. Furthermore, McConnell et al. (2008) found that physical attractiveness cues (e.g., being obese or slender, very good looking or normatively unattractive) had a substantial impact on one's implicit evaluations of a target individual, but not on conscious feelings toward the same person, and these evaluations are especially likely to direct behavior without one's awareness or intention (McConnell and Leibold 2001). Recently, John et al. (2011) showed that willingness to disclose personal information is situation specific and reliant on specific environmental cues that often bear little connection to or are even reversely related to objective hazards. Likewise, Lowry et al. (2012) showed that privacy assurance effectiveness is enhanced when seals and statements are accompanied by the unrelated variables of website quality and brand image.

Proposition D5. *Source variables, such as attractiveness, perceived authority, or perceived trustworthiness, can impact the APCO model constructs.*

Misattribution Effects. Closely related to the impact of peripheral cues, misattribution effects can lead people to inappropriate construals of influence settings. Misattributions occur when a person incorrectly ascribes an experience to a perceived cause and acts in accordance with this incorrect understanding of the situation (Bem 1967, Kahneman and Frederick 2002). For example, people standing on a precarious rope bridge will misattribute their physiological responses (e.g., increased heart rate) to a nearby attractive person and draw the conclusion that they are romantically interested in the person (e.g., misattributing their heart rate to the person rather than to the bridge), resulting in people asking the person out on a date (Dutton and Aron 1974). A very illustrative study of the power of misattribution was published by Risen and Critcher (2011), who found that just feeling warm makes people more likely to believe in global warming. The researchers conducted an indoor experiment in which the temperature was manipulated by a thermostat, which was clearly unrelated to a long-term climate trend. People in the warm room were more likely to believe in global warming than were the people in the colder room, revealing misattribution. In a similar study by Li et al. (2011a), respondents who thought that the day was warmer than usual believed more in and had a greater concern about global warming than

did respondents who thought that the day was colder than usual.

Depending on the specific effect and context, misattribution can have a powerful effect on trust, risk, benefits, privacy concerns, and behavioral reactions. If people experience pleasant feelings, they will look for the cause of their feelings and thus may misattribute them to any plausible object or outcome—for example, deeming an online "friend" as trustworthy and sending intimate pictures or sharing intimate secrets. One can just as easily misattribute negative feelings as well. This can be seen in online experiences that can be engineered to generate "shock value" to drive user clicks by, for example, showing vile and scary images that influence perceptions of risk and drive users to click and use a product or service that promises to prevent what is conveyed by the images.

Proposition D6. *Misattribution can impact the APCO model constructs.*

Anchoring. Individuals are sometimes unable to dismiss irrelevant information when making decisions (Ariely et al. 2003, 2006; Lehrer 2009; Tversky and Kahneman 1974). For example, before a bidding experiment, students were asked to write down the last two digits of their Social Security number. Then they were asked to write the maximum amount that they were willing to pay for the items. On average, students with a higher last two digits of their Social Security number were willing to spend 300% more than those with low numbers (Ariely et al. 2006). Anchoring is a common artifact used by salespeople and smart negotiators, where a starting point is suggested as an anchor to the decision-making process (Goes 2013). In fact, Adomavicius et al. (2013) showed that ratings from recommender systems can be used to anchor consumers' own preference ratings.

In privacy-related decision making, if people's perceptions of a disclosure request are anchored to a seemingly relevant but actually disconnected information set, they can form inaccurate perceptions of the behavioral alternatives as well as the risks and benefits of the disclosure. Although speculative, it is reasonable, for example, that anchoring a request for one's annual income to a seemingly unrelated request for one's license plate number could lead to a level of disclosure that the individual might—under other circumstances—dismiss. Similarly, the anchoring effect can impact trust, risk, perceptions of benefits, or behavioral reactions.

Proposition D7. *Anchoring people's choices to arbitrary coherence can impact the APCO model constructs.*

Herding Effect. The final cognitive limitation we address in this commentary is the *herding effect*, which refers to individuals acting together and being influenced by each other without thoughtful reasoning or planned direction. Herding behavior has been studied in the context of formation of attitudes and behavior in schools, riots, mob violence, strikes, religious gatherings, stock market bubbles, and everyday decision making such as choosing a restaurant. Recently published research (Muchnik et al. 2013) suggests that prior ratings of Web and social networking sites create significant bias in individual rating behavior.

In privacy-related studies, Acquisti et al. (2012) showed that subjects were more willing to divulge sensitive information when told that previous respondents have made sensitive disclosures. Thus, people's decisions to disclose personal information are competitive in nature. The researchers' results also seem to suggest that privacy concerns can also be influenced by comparative judgments.

Herding is consistent with broader low-effort processes involving social validation (Cialdini 2009), which refers to people adhering to an established norm because "others are doing it too." For example, having others establish a norm of trusting Facebook with location information can establish a default that leads new users to have the same trust without a thoughtful analysis of whether it is a sound privacy decision.

As with D4, the influences of herding effects will most likely be observed directly in behavioral reactions. However, it is conceivable that these biases could also influence some of the other APCO constructs.

Proposition D8. *Herding effects can impact the APCO model constructs.*

Rethinking APCO

We have outlined a number of propositions regarding indirect and direct effects that were not considered in extant models of privacy, including APCO. These factors appear to be important for explaining privacy-related behaviors, yet they have received little attention to date in the privacy research stream. We do not claim that this list of propositions is exhaustive. For example, other factors could conceivably impact the level of cognitive effort (P1–P4 in our enhanced model), which in turn would modify the existing APCO relations and the relative strength of the direct effects from peripheral cues, biases, heuristics, and misattribution effects on APCO constructs (D1–D8 in our enhanced model).

It is also clear that no single research study could possibly examine all of these moderation, mediation, moderated-mediation, and direct effects. As will be discussed below, many of the postulated relations in the enhanced APCO model are most appropriately tested in laboratory experiments, which, because of the need for controls and designed treatments, are limited

in the number of factors that can be simultaneously tested in any single study.

Additionally, researchers who attempt to test enhanced APCO propositions via surveys or field studies will inevitably confront the complexities of sorting through the nuanced relationships. Just as with the original APCO model, the enhanced model is best viewed as a macromodel that can guide research over a significant period of time. Even so, the enhanced model provides a multitude of exciting research opportunities, a topic to which we now turn.

New Research Paths

Our enhanced APCO model promotes a new and expanded research stream related to privacy—one that is almost bereft of published work heretofore. The enhanced APCO propositions can be examined through laboratory experiments, survey studies, or field experiments. Researchers should be cognizant of the sample population studied so that conclusions can be generalized appropriately and as broadly as possible. For example, exclusive use of undergraduate participants may be convenient in some cases, but their greater comfort with disclosing personal data in online contexts may render them less pliable in terms of manipulation of privacy concerns, and thus their choices may not generalize to older individuals who have different experiences with Internet use. When experimental controls are employed along with random assignment of subjects to treatment groups, the generalizability of the subject pool is of less concern as long as the subjects' salient attributes can be reasonably assumed to match those of the broader population of interest. Note, however, that tasks requiring organizational or political understanding are often inappropriate for student subjects, even in controlled experiments, because students cannot be expected to fully comprehend the scenarios and treatments. (See Compeau et al. 2012 for an in-depth discussion of the appropriate process for incorporating student subjects.)

One important implication from the analysis we offer in the enhanced APCO model involves the value of experimental methods in addition to correlational approaches; that is, because people cannot (by definition) report on their evaluations or on the influence of peripheral cues in their behavior, experimental methods that manipulate these influences while keeping all else constant offer the most effective path to evaluating and establishing their impact on behavior. Accordingly, experiments should be designed to capture actual subject behavior, rather than to ask respondents to answer questions about intended behaviors in hypothetical situations. The latter approach is not appropriate for testing the propositions in this paper. There will be a significant common methods bias, which can lead to nongeneralizable results.

The research propositions in the enhanced APCO model are stated at the individual unit of analysis, which is the level at which the underlying psychological theories provide the most salient guidance. However, as was noted by Bélanger and Crossler (2011), an exhaustive treatment of privacy-related issues must include multilevel analyses that also capture group-level, organizational, and societal phenomena. These propositions do not lend themselves immediately to qualitative research (especially, to process tracing) because of their unit of analysis. Therefore, examination of these specific propositions would not yield helpful insights into the understanding of episodes and encounters in a process context, and we suspect that most privacy researchers will prefer to examine these phenomena under more controlled conditions until we reach a higher plateau of understanding. We note, however, that researchers who are willing to consider and incorporate individuals' peripheral processing within organizational structures could ultimately yield some of the richest insights in this domain. For example, corporations or cultures certainly have expectations about who to trust or losses to be avoided that will drive privacy-related actions in these larger contexts.

Implications

Assuming that researchers extend the privacy stream as suggested above, there could be significant implications for individuals, organizations, and policy makers. We consider each.

Implications for Individuals

For individuals, the most important implication will be an increased need for *awareness* of heretofore little-discussed factors that may influence people's decision making. Few individuals are aware, for example, that their mood state may impact how they make decisions regarding the disclosure of personal information to online entities. Likewise, they have likely given little thought to some inherent biases that may alter their evaluation of important parameters associated with their handling of information and online commercial transactions.

Although the expanded research stream is a nascent one, savvy consumers will take steps to inoculate themselves against manipulations of affect and other factors that may influence the magnitude of their information processing, and they can be on guard for heuristics that bias their decisions about disclosing personal information. As the research stream grows, additional (and at present, unconsidered) insights will be gained, and alert consumers will take advantage of those insights so that they can take full advantage of data-based opportunities without taking unnecessary risks.

Implications for Organizations

Some two decades ago, Smith (1993, 1994) documented an organizational privacy management process that consisted of "drift" (in organizational policies and practices), an external threat, and reaction. During the "drift" period—the stage occupied by most organizations now in terms of their approach to the factors found in the expanded APCO model—organizations are said to be "wandering in the maze" (Smith 1993, p. 107). Some organizations have already taken advantage of some of the factors that lead to low-effort processing (e.g., affective states, as illustrated in our opening example), but only in a few situations, such as "scareware," has there to date been an "external threat" in the form of a consumer backlash or regulatory response, so there has been little organizational focus on such "threats" and reactions to them.

Based on past experience, as the research stream begins to incorporate these new factors into privacy decision-making models, research findings (and attendant media attention) will likely lead to an initially defensive reaction from organizations. This will quickly be followed by attention from policy makers (more likely initially in Europe and some other countries than in the United States; see the following section). Some firms may overreact by jettisoning applications that may ultimately have proven to be useful and legal. In our view, the best organizational perspective would instead be a proactive one: to begin assessing how the firm may be employing techniques based on any of the "extended APCO" factors in existing applications and to tread carefully in implementing future applications that employ those techniques.

Implications for Policy Makers

Since the 1970s, privacy-related regulations have been instituted in almost all developed nations (Smith 1994, 2001). These regulations are not monolithic, however, and there are now tensions between some countries—most notably the United States and countries within the European Union—regarding the appropriate approaches to privacy regulation. The general distinction between the two domains has been cynically summarized as, "[i]n Europe, privacy is viewed as a 'human rights' issue; in the U.S., it is more often seen as a matter for contractual negotiation" (Smith 2001, p. 13). Indeed, recent events (e.g., Robinson et al. 2014, *Wall Street Journal* 2014) suggest that certain transborder data flows between the United States and Europe may be restricted because of disagreements over appropriate levels of privacy protection for data subjects.

To date, most of the tensions have revolved around the collection of what is considered by some to be sensitive information (e.g., location-based tracking, online Web tracking). This focus can be traced largely to the publicity associated with widely promoted events in social media and the worldwide popularity of services such as Facebook and Instagram. Most of the perceived infractions that have been identified by regulatory authorities have been ones that are easily considered within the original APCO models—decisions based on use and reuse of consumer, geographical, and social data, often filtered through an inferred privacy calculus. To date, policy makers have rarely focused on possible uses (and perceived misuses) of affective factors or the exploitation of extraneous influences. However, as researchers begin exploring these new factors, it is likely that media attention will follow, and policy makers will become attuned to the ways in which firms may be taking advantage of these factors. Because many of these influences are "invisible" to logic and reasoning, their impact may be viewed as especially insidious. Thus, it can be expected that policy makers (first in Europe and other places that associate privacy with "human rights," and then later in countries such as the United States) will react to these emerging applications with alarm, and reactive regulation—with accompanying regulatory structures—can be expected to follow.

As with individuals and organizations, policy makers—especially those in the United States, which often seems to lag other developed nations in confronting privacy quandaries—would therefore be well advised to take steps to both understand the "outside the 'APCO' box" effects and to proactively anticipate both organizational applications and research findings that could increase demand for additional regulation.

Acknowledgments

The authors gratefully acknowledge the senior editor, associate editor, and three anonymous reviewers for their outstanding guidance as they revised this manuscript. Authors contributed equally and are listed in alphabetical order.

References

Acquisti A (2004) Privacy in electronic commerce and the economics of immediate gratification. *Proc. 5th ACM Electronic Commerce Conf.* (ACM, New York), 21–29.

Acquisti A, Grossklags J (2005) Privacy and rationality in individual decision making. *IEEE Security Privacy* 3(1):26–33.

Acquisti A, John L, Loewenstein G (2012) The impact of relative standards on the propensity to disclose. *J. Marketing Res.* 49(2):160–174.

Adomavicius G, Bockstedt JC, Curley SP, Zhang J (2013) Do recommender systems manipulate consumer preferences? A study of anchoring effects. *Inform. Systems Res.* 24(4):856–875.

Angst CM, Agarwal R (2009) Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quart.* 33(2):339–370.

Ariely D (2008) *Predictably Irrational* (HarperCollins, New York).

Ariely D (2009) The end of rational economics. *Harvard Bus. Rev.* 87(7/8):78–84.

Ariely D, Loewenstein G (2006) The heat of the moment: The effect of sexual arousal on sexual decision making. *J. Behav. Decision Making* 19(2):87–98.

Ariely D, Huber J, Wertenbroch K (2005) When do losses loom larger than gains? *J. Marketing Res.* 42(2):134–138.
Ariely D, Loewenstein G, Prelec D (2003) Coherent arbitrariness: Stable demand curves without stable preferences. *Quart. J. Econom.* 118(1):73–105.
Ariely D, Loewenstein G, Prelec D (2006) Tom Sawyer and the construction of value. *J. Econom. Behav. Organ.* 60(1):1–10.
Bansal G, Zahedi F, Gefen D (2008) The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *Proc. 29th Internat. Conf. Inform. Systems, Paris.*
Baron RS, Inman M, Kao C, Logan H (1992) Negative emotion and superficial social processing. *Motivation Emotion* 16(4):323–345.
Bélanger F, Crossler RE (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quart.* 35(4):1017–1041.
Bem DJ (1967) Self-perception: An alternative interpretation of cognitive dissonance phenomena. *Psych. Rev.* 74(3):183–200.
Bodenhausen GV, Mussweiler T, Gabriel S, Moreno KN (2001) *Affective Influences on Stereotyping and Intergroup Relations* (Erlbaum, Mahwah, NJ).
Brandimarte L, Acquisti A, Loewenstein G (2013) Misplaced confidences: Privacy and the control paradox. *Soc. Psych. Personality Sci.* 4(3):340–347.
Briñol P, Petty RE (2012) *The History of Attitudes and Persuasion Research* (Psychology Press, New York).
Cacioppo JT, Petty RE (1982) The need for cognition. *J. Personality Soc. Psych.* 42(1):116–131.
Cacioppo JT, Petty RE, Kao CF, Rodrigues R (1986) Central and peripheral routes to persuasion: An individual difference perspective. *J. Personality Soc. Psych.* 51(5):1032–1043.
Chaiken S (1978) The use of source versus message cues in persuasion: An information processing analysis. Unpublished doctoral dissertation, University of Massachusetts Amherst, Amherst.
Chaiken S (1980) Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *J. Personality Soc. Psych.* 39(5):752–766.
Cialdini RB (2009) *Influence: Science and Practice* (Pearson Education, Boston).
Compeau D, Marcolin B, Kelley H, Higgins C (2012) Research commentary—Generalizability of information systems using student subjects—A reflection on our practices and recommendations for future research. *Inform. Systems Res.* 23(4): 1093–1109.
Consumers Union (2008) Poll: Consumers concerned about Internet privacy. (September 25), http://consumersunion.org/news/poll-consumers-concerned-about-internet-privacy/.
Dennis AR, Robert LP, Curtis AM, Kowalczyk ST, Hasty BK (2012) Research note—Trust is in the eye of the beholder: A vignette study of postevent behavioral controls' effects on individual trust in virtual teams. *Inform. Systems Res.* 23(2):546–558.
Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inform. Systems Res.* 17(1):61–80.
Dutton DG, Aron AP (1974) Some evidence for heightened sexual attraction under conditions of high anxiety. *J. Personality Soc. Psych.* 30(4):510–517.
Eastlick MA, Lotz SL, Warrington P (2006) Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *J. Bus. Res.* 59(8):877–886.
Equifax (1995) *Equifax-Harris Mid-decade Consumer Privacy Survey 1995* (Equifax, New York).
Fang Y, Qureshi I, Sun H, McCole P, Ramsey E, Lim KH (2014) Trust, satisfaction, and online repurchase intention: The moderating role of perceived effectiveness of e-commerce institutional mechanisms. *MIS Quart.* 38(2):407–427.
Flynn FJ, Lake VKB (2008) If you need help, just ask: Underestimating compliance with direct requests for help. *J. Personality Soc. Psych.* 95(1):128–143.
Gefen D, Pavlou PA (2012) The boundaries of trust and risk: The quadratic moderating role of institutional structures. *Inform. Systems Res.* 23(3):940–959.
Gefen D, Wyss S, Lichtenstein Y (2008) Business familiarity as risk mitigation in software development outsourcing contracts. *MIS Quart.* 32(3):531–551.
Gilbert D (1991) How mental systems believe. *Amer. Psychologist* 46(2):107–119.
Gneezy U, Imas A (2014) Materazzi effect and the strategic use of anger in competitive interactions. *Proc. Natl. Acad. Sci. USA* 111(4):1334–1337.
Gneezy U, Imas A, Madarász K (2014) Conscience accounting: Emotion dynamics and social behavior. *Management Sci.* 60(11): 2645–2658.
Goes PB (2013) Information systems research and behavioral economics. *MIS Quart.* 37(3):iii–viii.
Grice P (1975) *Logic and Conversation* (Academic Press, New York).
Grossklags J, Acquisti A (2007) When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. *Proc. 6th Workshop Econom. Inform. Security, Pittsburgh.* http://weis07.infosecon.net/papers/66.pdf.
Harris Interactive (2011) Mobile privacy: A user's perspective. Accessed July 30, 2012, http://www.truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/.
Hong W, Thong JYL (2013) Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quart.* 37(1):275–298.
Hoorens V, Buunk BP (1993) Social comparison of health risks: Locus of control, the person-positivity bias, and unrealistic optimism. *J. Appl. Soc. Psych.* 23(4):291–302.
Jarvenpaa SL, Majchrzak A (2010) Research commentary—Vigilant interaction in knowledge collaboration: Challenges of online user participation under ambivalence. *Inform. Systems Res.* 21(4): 773–784.
Jarvenpaa SL, Shaw TR, Staples DS (2004) Toward contextualized theories of trust: The role of trust in global virtual teams. *Inform. Systems Res.* 15(3):250–267.
Jaswal VK, Croft AC, Setia AR, Cole CA (2010) Young children have a specific, highly robust bias to trust testimony. *Psych. Sci.* 21(10):1541–1547.
John L, Acquisti A, Loewenstein G (2011) Strangers on a plane: Context-dependent willingness to divulge sensitive information. *J. Consumer Res.* 37(5):858–873.
Johnston AC, Warkentin M (2010) Fear appeals and information security behaviors: An empirical study. *MIS Quart.* 34(3): 549–566.
Kahneman D, Frederick S (2002) *Representativeness Revisited: Attribute Substitution in Intuitive Judgment* (Cambridge University Press, New York).
Kahneman D, Tversky A (1979) Prospect theory: An analysis of decision under risk. *Econometrica* 47(2):263–292.
Kahneman D, Knetsch KL, Thaler RH (1991) Anomalies: The endowment effect, loss aversion, and status quo bias. *J. Econom. Perspect.* 5(1):193–206.
Kahneman D, Slovic P, Tversky A (1982) *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge University Press, New York).
Lee L, Amir O, Ariely D (2009) In search of homo economicus: Cognitive noise and the role of emotion in preference consistency. *J. Consumer Res.* 36(2):173–187.
Lehrer J (2009) *How We Decide* (Houghton Mifflin Harcourt, New York).
Levin IP, Schneider SL, Gaeth GJ (1998) All frames are not created equal: A typology and critical analysis of framing effects. *Organ. Behav. Human Decision Processes* 76(2):149–188.
Li H, Sarathy R, Xu H (2011b) The role of affect and cognition on the online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems* 51(3): 434–445.
Li H, Sarathy R, Zhang J (2008) The role of emotions in shaping consumers' privacy beliefs about unfamiliar online vendors. *J. Inform. Privacy Security* 4(3):36–62.
Li Y (2011) Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Comm. Assoc. Inform. Systems* 28(1):453–496.

Li Y, Johnson E, Zaval L (2011a) Local warming: Daily temperature change influences belief in global warming. *Psych. Sci.* 22(4): 454–459.

Liang H, Xue Y (2009) Avoidance of information technology threats: A theoretical perspective. *MIS Quart.* 33(1):71–90.

Lim ET, Tan C-W, Cyr D, Pan SL, Xiao B (2012) Advancing public trust relationships in electronic government: The Singapore e-filing journey. *Inform. Systems Res.* 23(4):1110–1130.

Liu BQ, Goodhue DL (2012) Two worlds of trust for potential e-commerce users: Humans as cognitive misers. *Inform. Systems Res.* 23(4):1246–1262.

Loewenstein G (1996) Out of control: Visceral influences on behavior. *Organ. Behav. Human Decision Processes* 65(3):272–292.

Lowry PJ, Moody GD, Vance A, Jensen M, Jenkins JL, Wells T (2012) Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *J. Amer. Soc. Inform. Sci. Tech.* 63(4):755–766.

McConnell AR, Leibold JM (2001) Relations among the implicit association test, discriminatory behavior, and explicit measures of racial attitudes. *J. Experiment. Soc. Psych.* 37(6):435–442.

McConnell AR, Rydell RJ (2014) *The Systems of Evaluation Model: A Dual-Systems Approach to Attitudes* (Guilford Press, New York).

McConnell AR, Rydell RJ, Strain LM, Mackie DM (2008) Forming implicit and explicit attitudes toward individuals: Social group association cues. *J. Personality Soc. Psych.* 94(5):792–807.

Metzger MJ (2004) Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *J. Comput.-Mediated Comm.* 9(4).

Möllering G (2006) *Trust: Reason, Routine, Reflexivity* (Elsevier, Oxford, UK).

Muchnik L, Aral S, Taylor SJ (2013) Social influence bias: A randomized experiment. *Science* 341(6146):647–651.

Newport F (2001) The fascinating "local versus national" phenomenon. Gallup (February 9), http://www.gallup.com/poll/4660/fascinating-local-versus-national-phenomenon.aspx.

Nicolaou AI, McKnight DH (2006) Perceived information quality in data exchanges: Effects on risk, trust, and intention to use. *Inform. Systems Res.* 17(4):332–351.

Novemsky N, Kahneman D (2005) The boundaries of loss aversion. *J. Marketing Res.* 42(2):119–128.

Ou CX, Pavlou PA, Davison RM (2014) Swift guanxi in online marketplaces: The role of computer-mediated communication technologies. *MIS Quart.* 38(1):209–230.

Özpolat K, Gao G, Jank K, Viswanathan S (2013) Research note—The value of third-party assurance seals in online retailing: An empirical investigation. *Inform. Systems Res.* 24(4):1100–1111.

Pavlou PA (2011) State of the information privacy literature: Where are we now and where should we go? *MIS Quart.* 35(4): 977–988.

Petty RE, Cacioppo JT (1981) *Attitudes and Persuasion: Classic and Contemporary Approaches* (William C. Brown, Dubuque, IA).

Petty RE, Cacioppo JT (1986) The elaboration likelihood model of persuasion. Berkowitz L, ed. *Advances in Experimental Social Psychology*, Vol. 19 (Elsevier, New York), 123–203.

Petty RE, Wegener DT (1998) *Attitude Change: Multiple Roles for Persuasion Variables* (McGraw-Hill, New York).

Piccoli G, Ives B (2003) Trust and the unintended effects of behavior control in virtual teams. *MIS Quart.* 27(3):365–395.

Polites GL, Karahanna E (2012) Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new systems acceptance. *MIS Quart.* 36(1):21–42.

Polites GL, Karahanna E (2013) The embeddedness of information systems habits in organizational and individual level routines: Development and disruption. *MIS Quart.* 37(1):221–246.

Pratt TC, Cullen FT (2000) The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology* 38(3):931–964.

Preacher KJ, Rucker DD, Hayes AF (2007) Addressing moderated mediation hypotheses: Theory, methods, and prescriptions. *Multivariate Behavioral Res.* 42(1):185–227.

Priester JR, Petty RE (1995) Source attribution and persuasion: Perceived honesty as a determinant of message scrutiny. *Personality Soc. Psych. Bull.* 21(6):637–654.

Rice SC (2012) Reputation and uncertainty in online markets: An experimental study. *Inform. Systems Res.* 23(2):436–452.

Riedl R, Hubert M, Kenning P (2010) Are there neural gender differences in online trust? An fMRI study on the perceived trustworthiness of eBay offers. *MIS Quart.* 34(2):397–428.

Risen J, Critcher C (2011) Visceral fit: While in a visceral state, associated states of the world seem more likely. *J. Personality Soc. Psych.* 100(5):777–793.

Robinson F, Schechner S, Mizroch A (2014) EU orders Google to let users erase past. *Wall Street Journal* (May 13), http://www.wsj.com/articles/SB10001424052702303851804579559280623224964.

Rogers RW (1983) *Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation* (Guilford Press, New York).

Rustagi S, King WR, Kirsch L (2008) Predictors of formal control usage in IT outsourcing partnerships. *Inform. Systems Res.* 19(2):126–143.

Schoenbachler DD, Gordon GL (2002) Trust and customer willingness to provide information in database-driven relationship marketing. *J. Interactive Marketing* 16(3):2–16.

Schwarz N, Clore GL (2007) *Feelings and Phenomenal Experiences* (Guilford, New York).

Sears D (1983) The person-positivity bias. *J. Personality Soc. Psych.* 44(2):233–250.

Shampanier K, Mazar N, Ariely D (2007) How small is zero price? The true value of free products. *Marketing Sci.* 26(6):742–757.

Sharot T (2011) *The Optimism Bias: A Tour of the Irrationally Positive Brain* (Pantheon Books, New York).

Shiv B, Fedorikhin A (1999) Heart and mind in conflict: The interplay of affect and cognition in consumer decision making. *J. Consumer Res.* 26(3):278–292.

Shiv B, Loewenstein G, Bechata A, Damasio H, Damasio AR (2005) Investment behavior and the negative side of emotion. *Psych. Sci.* 16(6):435–439.

Simpson S, Piquero N, Paternoster R (2002) *Rationality and Corporate Offending Decisions* (Routledge, New York).

Smith HJ (1993) Privacy policies and practices: Inside the organizational maze. *Comm. ACM* 36(12):105–122.

Smith HJ (1994) *Managing Privacy: Information Technology and Corporate America* (University of North Carolina Press, Chapel Hill, NC).

Smith HJ (2001) Information privacy and marketing: What the US should (and shouldn't) learn from Europe. *California Management Rev.* 43(2):8–33.

Smith HJ, Dinev T, Xu H (2011) Information privacy research: An interdisciplinary review. *MIS Quart.* 35(4):989–1015.

Smith SM, Levin IP (1996) Need for cognition and choice framing effects. *J. Behav. Decision Making* 9(4):283–290.

Sobel LA (1976) *War on Privacy* (Facts on File, New York).

Stoutenborough JS (2008) *Encyclopedia of Survey Research Methods* (Sage, Beverly Hills, CA).

Strack F, Schwarz N (1992) *Communicative Influences in Standardized Question Situations: The Case of Implicit Collaboration* (Sage, Beverly Hills, CA).

Taylor SE, Brown JD (1988) Illusion and well-being: A social psychological perspective on mental health. *Psych. Bull.* 103(2):193–210.

Tsai JY, Egelman S, Cranor L, Acquisti A (2011) The effect of online privacy information on purchasing behavior: An experiment study. *Inform. Systems Res.* 22(2):254–268.

Tversky A, Kahneman D (1974) Judgment under uncertainty: Heuristics and biases. *Science* 185(1124):1128–1130.

Tversky A, Kahneman D (1981) The framing of decisions and the psychology of choice. *Science* 211(4481):453–458.

Tversky A, Kahneman D (1991) Loss aversion in riskless choice: A reference-dependent model. *Quart. J. Econom.* 106(4):1039–1061.

Wall Street Journal (2014) The morning risk report: EU ruling on Google is a "game changer," attorney says. (May 14), http://blogs.wsj.com/riskandcompliance/2014/05/14/the-morning-risk-report-eu-ruling-on-google-is-a-game-changer/.

Westin AF (1967) *Privacy and Freedom* (Atheneum, New York).

Xu H, Teo HH, Tan BC (2005) Predicting the adoption of location-based services: The roles of trust and privacy risk. *Proc. 26th Ann. Internat. Conf. Inform. Systems, Las Vegas, NV*, 897–910.

Xu H, Teo HH, Tan BCY, Agarwal R (2010) The role of push-pull technology in privacy calculus: The case of location-based services. *J. Management Inform. Systems* 26(3):137–176.

Zhang P (2013) The affective response model: A theoretical framework of affective concepts and their relationships in the ICT context. *MIS Quart.* 37(1):247–274.

Zhang Y, Buda R (1999) Moderating effects of need for cognition on responses to positively versus negatively framed advertising messages. *J. Advertising* 28(2):1–15.