MIS Quarterly

RESEARCH ARTICLE

INCREASING ACCOUNTABILITY THROUGH USER-INTERFACE DESIGN ARTIFACTS: A NEW APPROACH TO ADDRESSING THE PROBLEM OF ACCESS-POLICY VIOLATIONS[1]

Anthony Vance
Information Systems Department, Marriott School of Management, Brigham Young University,
Provo, UT 84602 U.S.A. {anthony@vance.name}

Paul Benjamin Lowry
College of Business, City University of Hong Kong, 83 Tat Chee Avenue,
Kowloon Tong, Hong Kong CHINA {Paul.Lowry.PhD@gmail.com}

Dennis Eggett
Department of Statistics, Brigham Young University, Provo, UT 84602 U.S.A. {theegg@stat.byu.edu}

Access-policy violations are a growing problem with substantial costs for organizations. Although training programs and sanctions have been suggested as a means of reducing these violations, evidence shows the problem persists. It is thus imperative to identify additional ways to reduce access-policy violations, especially for systems providing broad access to data. We use accountability theory to develop four user-interface (UI) design artifacts that raise users' accountability perceptions within systems and in turn decrease access-policy violations. To test our model, we uniquely applied the scenario-based factorial survey method to various graphical manipulations of a records system containing sensitive information at a large organization with over 300 end users who use the system daily. We show that the UI design artifacts corresponding to four submanipulations of accountability can raise accountability and reduce access policy violation intentions. Our findings have several theoretical and practical implications for increasing accountability using UI design. Moreover, we are the first to extend the scenario-based factorial survey method to test design artifacts. This method provides the ability to use more design manipulations and to test with fewer users than is required in traditional experimentation and research on human–computer interaction. We also provide bootstrapping tests of mediation and moderation and demonstrate how to analyze fixed and random effects within the factorial survey method optimally.

Keywords: Accountability theory, identifiability, expectation of evaluation, awareness of monitoring, social presence, factorial survey method, user-interface design, information security policy violations, unauthorized access, mediation, moderation

[1]France Bélanger was the accepting senior editor for this paper. Merrill Warkentin served as the associate editor.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

Introduction

System access-policy violations by employees represent a growing problem that creates tremendous risks and costs for organizations. *Access-policy violations* occur when insiders access sensitive information contrary to the policies of their organizations (Ward and Smith 2002). These data breaches can result in identity theft, fraud, theft of intellectual property, and major financial consequences. In fact, employees are responsible for nearly half of all security violations and system intrusions (Crossler et al. 2013). Partially due to these issues, organizations spend substantial sums of money on internal information technology (IT) security and controls—many of which are aimed at employees (Crossler et al. 2013). However, technical solutions for restricting access privileges have limited power to stem the rising tide of violations. The problem of access-policy violations is exacerbated by the fact that many systems require broad-access privileges (i.e., *broad-access systems*). Not every system can be tightly controlled without placing inordinate constraints on employees' ability to perform their work. Unfortunately, this trade-off opens organizations to serious security risks.

For example, in health care, broad-access systems have led to extensive privacy violations and "data hemorrhages" in which highly confidential information is unintentionally and intentionally leaked—leading to privacy violations, identity theft, and legal settlements that cost the U.S. health-care sector an estimated US$6 billion per year (Johnson and Willey 2011). As an indication of this problem, the U.S. Department of Health and Human Services, which monitors compliance with the Health Insurance Portability and Accountability Act rules, receives nearly 10,000 privacy violation complaints each year. In response, in 2009 the U.S. Health Information Technology for Economic and Clinical Health Act was passed; it assesses penalties of up to US$1.5 million for health-care providers for the misuse of private health information.

The cases of the former U.S. Army Private Manning and of Edward Snowden are emblematic examples of the impact of access-policy violations. Before Manning's unauthorized disclosure of more than 250,000 U.S. diplomatic cables to WikiLeaks, approximately 2.5 million military and civilian users had access to the Secret Internet Protocol Router Network, a private government network for sharing classified information. The threat of an insider disclosing sensitive information was considered "the cost of doing business," that is, of sharing information freely among agencies. However, following the embarrassing and staggeringly large loss of classified information due to access-policy violations, the U.S. government issued an executive order to revise its operational security policies to substantially limit access to classified information. Edward Snowden parlayed his access as a system administrator for the U.S. National Security Agency (NSA) to leak an estimated 1.7 million classified documents, the largest intelligence breach in U.S. history. In response, the NSA has implemented a "two-man rule" to control access to sensitive information and is seeking to dramatically reduce the number of system administrators who receive broad-access privileges. In both cases, the downside to the solutions is that access restrictions greatly hamper the work of millions of government employees dealing with classified information in real time, thus giving rise to increased costs and other problems. Health-care institutions confront the same problem, because broad access is required to solve many medical problems.

Traditionally, two fairly obtrusive and time-consuming interventions have been used to decrease access-policy violations (D'Arcy et al. 2009): (1) using sanctions, as recommended by deterrence theory (DT), and (2) providing ongoing security education, training, and awareness (SETA) programs. Although these approaches are valuable, access-policy violations persist even when sanctions and regular training are instituted. Another problem with DT–based approaches is that they rely on research founded in criminology and thus focus on leveraging the severity, swiftness, and certainty of threatened sanctions to scare employees away from deviant behavior (D'Arcy and Herath 2011). Such heavy-handed deterrence techniques have inconsistent results in the workplace (D'Arcy and Herath 2011). Worse, such approaches can cause low morale in a professional work environment or may prompt employees to lash out and even do the opposite of what the policy states (Lowry and Moody 2015; Lowry, Teh, et al. 2010; Posey et al. 2011). Hence, it is imperative to identify additional techniques for thwarting access-policy violations, beyond sanctions and SETA programs (Crossler et al. 2013).

Recent work has pointed to the potential usefulness of perceptions of *accountability*, "the implicit or explicit pressure to justify one's beliefs and actions to others" (Tadmor and Tetlock 2009, p. 8), for deterring access-policy violations (Vance et al. 2013). Other research has also suggested that end-user usability design issues can be a root cause of data hemorrhaging (Johnson and Willey 2011). Using a design approach to thwart these issues is particularly intriguing because it is less invasive than deterrence approaches. We thus move beyond traditional approaches of overtly encouraging security compliance to considerations of how elements of user-interface (UI) design can be used to noninvasively encourage security compliance. These possibilities lead to the following research questions:

RQ1. *How can UI design artifacts increase perceptions of accountability in the users of a broad-access system?*

RQ2. *Can increases in user accountability reduce intentions to violate access policies?*

RQ3. *Does accountability mediate the effect of UI design artifacts on the intention to violate the access policy?*

We investigated these research questions using a novel graphical application of the factorial survey method (Jasso 2006). Additionally, we tested our accountability model using a sample of 318 actual employees who routinely use a specific broad-access system. This focus on a particular real-world organizational context allowed us to evaluate the effectiveness of four UI design artifacts that we designed specifically for use with the selected broad-access system. We found that accountability directly influences intention to violate the access policy. We also found that accountability mediates the effects of our UI design artifacts on intention to violate the access policy. This finding is intriguing, particularly because it opens the door to approaches to curbing access-policy violations that are less coercive than traditional deterrence approaches.

To proceed, we provide an overview of our research model and present some background on accountability. We then propose our theoretical model and related hypotheses. Subsequently, we describe our application of the factorial survey method and analysis of our field data. Finally, we discuss the contributions of this study and suggest areas of future research on using accountability to reduce access-policy violations.

Accountability User-Interface Design Artifacts and Hypotheses

Building on the work of Vance et al. (2013), we explain how UI design artifacts can be manipulated to increase accountability and thus decrease the intention to violate organizational access policies. Figure 1 depicts our model, which predicts that four constructs that can be operationalized as UI design artifacts—identifiability, expectation of evaluation, awareness of monitoring, and social presence—will increase accountability. In turn, accountability will mediate the effects of these UI artifacts on the intention to commit access-policy violations. Finally, we predict that the UI artifacts will interact to decrease the intention to violate access policies.

The Construct of Accountability

A challenge of studying accountability is that the concept is used broadly in a variety of fields, including psychology, philosophy, ethics, political science, and organizational behavior, and can be applied at both the individual and organizational level. Bovens (2010) distinguishes between the two most prevalent uses of accountability: as a virtue and as a mechanism. As a *virtue*, accountability is considered desirable in public officials, government agencies, and firms; hence, in this context, accountability is a positive feature of an entity. As a *mechanism*, accountability is a process in which a person has a potential obligation to explain his/her actions to another party who has the right to pass judgment on those actions and to administer potential positive or negative consequences in response to them. Bovens' definition of accountability as a mechanism is almost identical to the definition given and used by Tetlock and various coauthors (Tetlock 1983a, 1983b, 1985, 1992, 1999; Tetlock and Boettger 1989, 1994; Tetlock and Kim 1987; Tetlock et al. 1989). We embrace this definition because such mechanisms are typical in employee–manager relationships (Bovens 2010).

Accountability is therefore a key form of organizational governance that cannot exist without mechanisms that promote it. The traditional mechanisms of accountability are overt expectations of evaluation and awareness of monitoring. This understanding of accountability has some conceptual overlap with DT, although there are important differences (Appendix A).

Accountability Theory

Accountability theory explains how the perceived need to justify one's behaviors to another party causes one to consider and feel accountable for the process by which decisions and judgments have been reached. In turn, this perceived need to account for a decision-making process and outcome increases the likelihood that one will think deeply and systematically about one's procedural behaviors. In cognitive psychology, this principle has long been known as systematic processing (Crano and Prislin 2006).

Systematic processing involves the use of deep cognitive processing and elaboration to make decisions (Chaiken and Maheswaran 1994; Lowry et al. 2012). People who think systematically in making decisions about systems use will consider more inputs and think more carefully to derive an optimal decision that they uniquely own (Lowry et al. 2012). Thus, they will go through a "thorough, in-depth, complete, and well-advised processing of all given information" in making optimal decisions (Wirth et al. 2007, p. 780). An increased focus on systematic processing consequently heightens the emphasis on creating effective outcomes for which the person is accountable (Scholten et al. 2007). Given that its connection to accountability is established in the literature, we do not examine systematic processing directly;

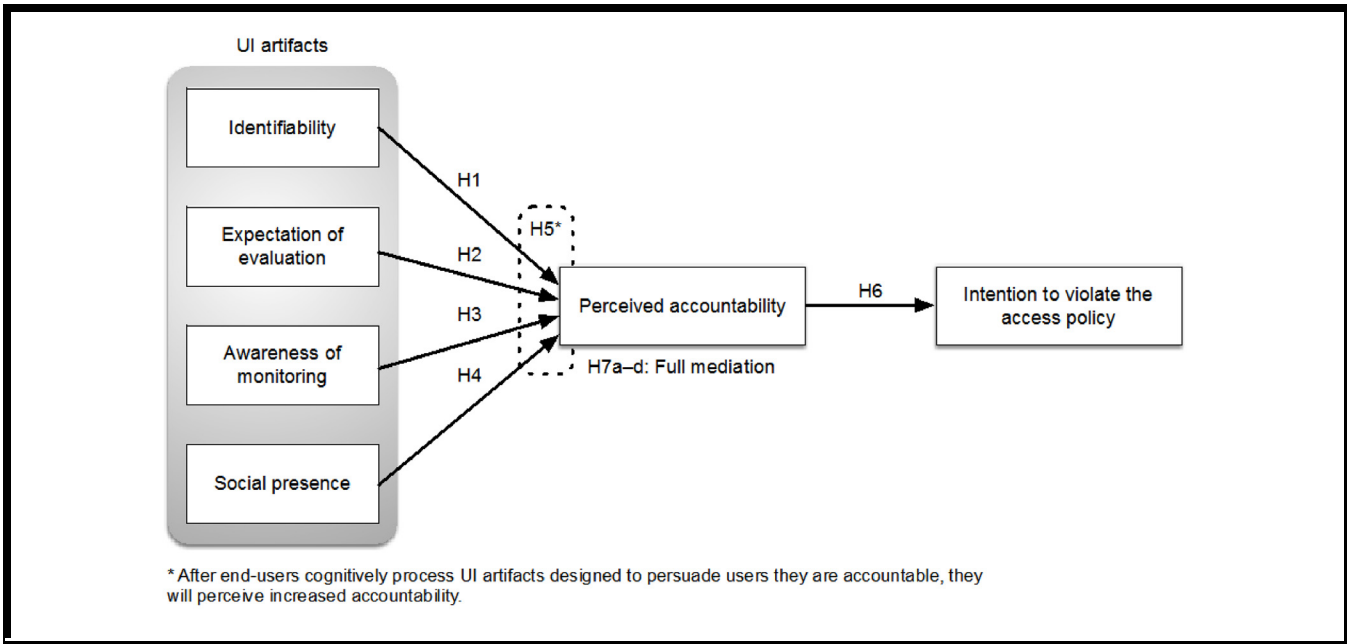

Figure 1. Proposed Accountability Model

rather, it is an assumption of our model: users who engage in systematic processing are more likely to consider the factual consequences of their use and thus will perceive higher accountability for their actions than those engaging in *heuristic processing*.[2]

The increased decision-making awareness fostered by systematic processing attaches a sense of accountability to processes and outcomes that can increase prosocial behaviors (Fandt and Ferris 1990), increase conformity to expected behaviors (Tetlock et al. 1989), increase conservatism (Staw 1976), and decrease risk taking (Schlenker et al. 1991). In organizational contexts, negative emotions such as anger and anxiety can increase nonsystematic processing, which results in greater risk taking and deviant behavior (Rodell and Judge 2009).

Accountability theory proposes several mechanisms that increase accountability perceptions. For example, "even the simplest accountability manipulation necessarily implicates several empirically distinguishable submanipulations" (Lerner and Tetlock 1999, p. 255), including the presence of another person, identifiability, and expectation of evaluation. Recent research has shown that text-based scenarios can manipulate the four core components of accountability theory (Vance et al. 2013) on which we build (1) identifiability, (2) expectation of evaluation, (3) awareness of monitoring, and (4) social presence.

Identifiability and Accountability

Identifiability is a person's "knowledge that his outputs could be linked to him" and thus reveal his/her true identity (Williams et al. 1981, p. 309), which is in direct contrast to anonymity (Schopler et al. 1995). Due to this self-linkage, identifiability is a potent deterrent of antisocial behaviors such as social loafing, flaming, and group discontinuities. This deterrent effect occurs because people modify their behavior if they believe their identity might be recognized (Reicher and Levine 1994).

Identifiability is closely related to the construct of *individuation*, a person's belief that his/her actions within a group can be associated with him/her individually (Reicher and Levine 1994). Studies have found that when people feel *deindividuated*, they are less restrained in their normal behaviors (Reicher and Levine 1994). In our context, the mere use of computers to communicate—even if the user is identified—leads to deindividuation, because computer use can lead to a sense of "disembodiment" in users as a result of its mediation effect (Tanis and Postmes 2007). Conversely, when individ-

[2] *Heuristic processing* occurs when "lack of ability and/or motivation causes individuals to evaluate messages by following the peripheral route of persuasion that involves 'shallow' information processing and the use of shortcuts, heuristics, and emotions for decision-making....These shortcuts focus away from the message and toward more superficial attributes of the source or message" (Lowry et al. 2012, p. 758).

uals sense that they are individuated—that is, distinguishable within a group—antisocial behaviors are curtailed (Reicher and Levine 1994). A classic example from the social psychology literature shows that children trick-or-treating alone are much less likely to take more than their fair share of candy than those doing so in groups (Diener et al. 1976). Likewise, end users who perceive increased *identifiability* should have an increased sense of accountability (*P1*).

Research on human–computer interaction (HCI) has investigated *cues to identity*, UI design artifacts that reveal or give correct personal information about a user that can be linked to the user. Tanis and Postmes (2007) have effectively manipulated digital photographs of participants and personal information experimentally and found that these increased individuation. In similar studies (Tanis and Postmes 2003; Walther et al. 2001), photographs have been shown to be effective cues to identity because humans have a highly evolved sensitivity to recognizing facial appearance (Mondloch and Desjarlais 2010).[3]

Consequently, identifiability implemented in UI design artifacts should increase accountability, whereas lack of identifiability should decrease accountability. Identifiability is an important facilitator of accountability, because individuals who perceive increased identifiability know their actions can be linked to them personally and that they can therefore be made responsible for those actions (Lerner and Tetlock 1999). Hence, when individuals are performing identifiable behaviors, they are more likely to engage in systematic processing to ensure that they perform only those behaviors for which they are willing to bear responsibility. We thus predict that the more identifiability features are built into a broad-access system, the greater the system users' perception of accountability will be. For example, if a user's photograph, name, and user ID are displayed when he/she is logged into a system, he/she will experience more identifiability and individuation. The associated increase in cognition and corresponding systematic processing should elicit an increased sense of accountability in users.

Notably, identifiability is not a binary concept (e.g., identified versus unidentified). Whereas to some extent the other constructs of accountability (such as expectation of evaluation) communicate to users that they are identified, the psychological impact of identifiability can be further strengthened by targeting users' identities more directly. For example, if users see their photograph, name, and user ID when they log into a system, they will perceive more identifiability and individuation as compared with merely seeing a history of their recent login attempts. We thus predict that the more identifiability features are built into a system, the greater the system users' perception of accountability will be. The associated increase in cognition and corresponding systematic processing should elicit an increased sense of accountability in users.

H1. *UI artifacts that manipulate identifiability will increase accountability.*

Expectation of Evaluation and Accountability

Expectation of evaluation is the belief that one's "performance will be assessed by another [party] according to some normative ground rules and with some implied consequences" (Lerner and Tetlock 1999, p. 255). These expectations increase socially desirable behaviors (Hochwarter et al. 2007; Lerner and Tetlock 1999) and deter socially undesirable ones (Sedikides et al. 2002). This link exists because the expectation of evaluation can create *evaluation apprehension*, a state of mind in which self-focused attention and cognitive anxiety are increased and influence a person toward socially desirable behavior because of previously learned social norms involving what is and is not acceptable behavior (Geen 1991).

Evaluation apprehension is typically cast in a negative light in the literature, but it is useful for creating accountability. In behavioral psychology, it can create experimental confounds in which participants provide socially desired but dishonest answers, especially when dealing with topics of great controversy and potential social shame (Cottrell 1972; Rosenberg 1968). Moreover, in collaborative creative tasks, evaluation apprehension can create group-process losses such as conformity or groupthink that undermine creative results (Lowry et al. 2005; Roberts et al. 2006). However, evaluation apprehension can be a positive force in an individual-level account-

[3]The communication cue of one's voice is also an important cue to identity (Sia et al. 2002) and is a critical component of natural communication (Kock 2004). This cue can be provided through voice conferencing or video conference capabilities (Kock 2004) or other forms of digitized voice. Other ways to invoke individuation through interface design include identifying who made what comments and indicating to which group a person belongs (Kahai 2009), as well as supplying biographical information (Tanis and Postmes 2003).

Conversely, several interface designs invoke deindividuation. Chief among these is allowing for anonymous logins or use of pseudonyms, the use of shared group logins, and any other features that focus on group contributions without individual identification, such as electronic brainstorming (Pinsonneault and Barki 1999). Use of altered or manipulated photographs that misrepresent actual physical appearance would likely raise similar issues, because humans are very adept at recognizing even the subtlest facial features (Mondloch and Desjarlais 2010). In addition, features that allow users to take on alter egos via avatars that misrepresent who they are (e.g., animal avatars) should also result in deindividuation

ability context such as ours. In this cognitive state, self-focus heightens the awareness of discrepancies between one's behaviors and normative standards (Sedikides et al. 2002). Also, the need to convey a good impression of oneself to others demands avoidance of negative evaluations that would undermine self-presentation efforts (Baumeister 1982). In summary, end users who perceive increased *expectation of evaluation* should have an increased sense of accountability (*P2*).

Based on accountability theory (Lerner and Tetlock 1999), we posit that the key element of invoking the expectation of evaluation is showing not just that transactions are logged visually, but that some kind of performance evaluation is occurring (or is likely to occur) based on user data. A user's awareness of such an interface should thus invoke evaluation apprehension that engages systematic processing and accountability. We thus propose that *expectation of evaluation*, which fosters evaluation apprehension, can be visually incorporated by depicting evidence of evaluation-based web log mining, transaction auditing, real-time reports of end-user activity, performance-based or exception-based visual dashboards of user activity, and so on. For example, seeing a visual audit trail indicating that others in the system have been audited for their system behavior naturally enhances one's expectation of being evaluated for similar behavior. The increase in cognition and systematic processing created by this expectation should help persuade users toward increased accountability. Thus, we predict the following:

H2. *UI artifacts that manipulate expectation of evaluation will increase accountability.*

Awareness of Monitoring and Accountability

Notably, much of the information used to foster the expectation of evaluation comes from the process of monitoring. *Monitoring* is the process of watching or tracking a user's activities (Griffith 1993). Computer-based monitoring can be particularly effective for transactions because systems can record transactions down to the granular level (Griffith 1993). Although the expectation of evaluation and awareness of monitoring are conceptually distinct, they naturally complement each other (Griffith 1993; Vance et al. 2013). For example, monitoring, evaluation, and enforcement are used in system-based audits to encourage adherence to data protection laws. Researchers have even developed a natural language that can be used to create privacy policies, which can then be automatically monitored and audited throughout an organization (Karat et al. 2005). Monitoring has been used in information security policy (ISP) compliance contexts to encourage ISP compliance (Boss et al. 2009; Herath and Rao 2009) and adherence to general computing policies (D'Arcy et al. 2009; Galletta and Hufnagel 1992). Such monitoring activities are more effective when incorporated into the normal ISP to make insiders aware that they will be monitored for their compliance actions (Boss et al. 2009). Thus, monitoring is more effective if there is *awareness of monitoring*, a user's state of active cognition that his/her system-related work is monitored. In summary, end users who perceive increased *awareness of monitoring* should have an increased sense of accountability (*P3*).

Monitoring awareness is normally accomplished through ISPs, training, or both (Boss et al. 2009; Herath and Rao 2009). We demonstrate that these mechanisms can be further represented as UI design artifacts that heighten one's belief that one's behavior is being monitored. Based on a review of the literature, we propose that visually depicting indications that the user is being monitored will increase the user's expectation that he/she is accountable. *Awareness of monitoring* can be visually incorporated by using history features such as breadcrumb trails, transaction logs, visual depictions of data history/web logs, and the like. For example, if a system shows complete visual logs of users' record-level behavior in a system (e.g., updates, deletion, access) and of when these events occurred, users will likely have an increased awareness of monitoring that increases their cognition and systematic processing and thus persuades them toward increased accountability. Thus, we predict the following:

H3. *UI artifacts that manipulate awareness of monitoring will increase accountability.*

Social Presence and Accountability

Social presence is the awareness of other users in the system (Walther 1992). Lerner and Tetlock (1999) identify the "mere presence of another" as an empirically distinguishable submanipulation of accountability, a claim supported by extensive research regarding the effects of the presence of another individual. Numerous experiments have shown that in the presence of an observer, a person suppresses behaviors that are viewed as socially unacceptable or that could invite disapproval (McLean et al. 1991). Guerin (1986) and Bond and Titus (1983) have performed large meta-analyses of the "mere presence" effect and found that individuals exhibit increased conforming behavior in the presence of another person, even when that person is not immediately present and cannot be observed.

Zajonc (1980) suggests that increased conformity in the presence of another is a product of uncertainty. Because the

presence of another implies the potential for interaction, a person must be prepared to react and respond to potential changes in the social environment. Because being called upon to justify one's actions to another (accountability) is a possible, albeit uncertain, outcome of interaction, one is more likely to feel the need to be prepared to respond than if no presence exists (Lerner and Tetlock 1999). In summary, the mere presence of another (i.e., *social presence*) should increase accountability and decrease the intention to violate social norms, and thus should often inhibit socially undesirable behavior (*P4*).

In a study of the effects of social presence (or lack thereof) with computer-mediated communication (CMC), Sia et al. (2002) show that CMC combined with anonymity leads to greater *group polarization*, in which a group takes a more extreme position or engages in more extreme thinking following group discussion than it would otherwise. They argue that group polarization is created partially due to anonymity and partially due to the removal of verbal cues, but most strongly due to the removal of visual cues that promote social presence. Lowry, Roberts et al. (2009) show that even with the use of anonymity, small, anonymous groups using a shared group editor (and thus experiencing social presence and awareness of others) achieved more implicit coordination and higher levels of productivity and quality than anonymous groups without such social presence. Another study demonstrates a link between awareness and accountability to others in massively multiplayer online worlds (Moore et al. 2007). Meanwhile, the need for presence or awareness has been widely demonstrated and successfully implemented in online social networking research (Lowry et al. 2011). Hence, the positive effects of social presence appear to hold in the digital realm.

Presence, which from an HCI standpoint is often referred to as *telepresence*, can be incorporated into the design of UI artifacts in several other ways (Deml 2007). For example, in instant messaging, presence is evoked by indicators of whether someone is online and available to chat and by similar awareness features (Lowry et al. 2011). Virtual reality can also increase a sense of presence (Suh and Lee 2005)—for example, by using more sophisticated mixed-reality systems (Liverani et al. 2006), collaborative virtual reality (Argelaguet et al. 2011), and virtual worlds, where social presence is more deeply embodied than in most other interactive environments (Mueller et al. 2011). 3D avatars that represent people online can also help increase a sense of presence (Qiu and Benbasat 2005), especially in an embodied virtual world context (Mennecke et al. 2011). Although it is unlikely that text-to-speech capabilities are as useful as live voice, they have been shown to increase the sense of presence in online interactions (Qiu and Benbasat 2005).

If a user can view an online activity screen depicting colleagues who are logged in and their activities, and can even view their screens, the user should have an increased sense of social presence. As noted, this awareness of others increases cognition and the systematic processing one might undertake to account for one's behaviors to others—thereby persuading one toward increased accountability. Thus, we predict the following:

H4. *UI artifacts that manipulate social presence will increase accountability.*

Using UI Design Artifacts to Increase Accountability

A core theoretical premise of this study is that UIs can be used to affect cognition and subsequent behavior. These assumptions are core principles of HCI research that have been extended into IS research; they are supported by many studies and are foundational principles of the stimulus–response phenomenon, in which UIs act as a stimulus (Zhang and Galletta 2006). End users have consistently been shown to notice and cognitively process UIs either systematically (e.g., if they are engaged, if the interface interaction is part of their work, and so on) or unsystematically (e.g., if they are disengaged or if they have no particular purpose for the interaction) (Lowry et al. 2012). Thus, interfaces can directly affect cognitive processing and subsequent persuasion (Lowry et al. 2012; Lowry, Wilson and Haig 2014). Thus, we predict the following:

H5. *UI artifacts that manipulate accountability mechanisms will increase accountability.*

Accountability and Access-Policy Violations

Based on our previous explanation of the causal mechanisms of accountability, we posit that those who perceive themselves to be accountable for the use of their access rights will be more likely to achieve a cognitive awareness that will increase conservative and prosocial behaviors. Such accountable end users will be less likely to commit access-policy violations than those who feel less accountable. Likewise, accountable end users will be less likely to make decisions based on emotions and nonsystematic processing that could cloud their judgment of optimal outcomes—that is, they will be less likely to take unnecessary risks with access-policy violations. In summary, we predict the following:

H6. *Perceived accountability decreases intention to commit access-policy violations.*

Accountability as a Mediator Between UI Design Artifacts and Intentions

We now explain why accountability mediates the effects of the UI design artifacts on the intention to commit access-policy violations. Mediation occurs when "an independent variable (X) causes an intervening variable (I), which in turn causes the dependent variable (Y)" (MacKinnon et al. 2002, p. 83). Mediation models are commonly used in the social sciences because they allow researchers to improve their explanations of associations by analyzing them into a chain of causal components (Shrout and Bolger 2002). Thus, such models work well in conjunction with causal theoretical models. Mediation models can enable researchers to "identify fundamental processes underlying human behavior that are relevant across behaviors and contexts" (MacKinnon and Fairchild 2009, p. 16). Further, once mediating variables are identified, interventions can be designed that efficiently target the variables in the mediated causal process (Shrout and Bolger 2002). As the IS discipline has matured, it has increasingly made use of mediation models (e.g., Burton-Jones and Hubona 2006; Lowry, Romano, et al. 2009).

We propose that accountability will mediate the effects of the UI design artifacts on the intention to commit access-policy violations. This mediation relationship should exist because identifiability, expectation of evaluation, awareness of monitoring, and social presence impact accountability, which in turn influences intentions and subsequent behavior (Lerner and Tetlock 1999). Accordingly, our mediated model presents a causal theoretical chain (Kenny 2008) in which the UI design artifacts increase accountability, which in turn reduces negative intentions. Recall that the extensive accountability literature notes that accountability arises from cognitive attitude and belief formation, as explained in the materials leading to H2. According to the extensive attitude-formation literature, intentions can be formed only after attitudes formation and beliefs formation, which are driven by cognitive processing (e.g., systematic or heuristic processing). Scores of cognitive psychology studies have shown that attitude formation drives persuasion and forms constructs such as intentions, which process is the foundation of virtually all information processing models (Crano and Prislin 2006). Intentions can never be formed before attitudes and beliefs. If this conclusion holds, then accountability is a cognitive mediator of intentions. Moreover, the mere presence of the UI design artifacts cannot reduce intention. The artifacts must cause an end user to engage in the systematic processing that increases accountability (Scholten et al. 2007), which then reduces the intention to commit access-policy violations.

H7. *Accountability will mediate the effects of UI artifacts for (1) identifiability, (2) expectation of evaluation, (3) awareness of monitoring, and (4) social presence on intention to commit access-policy violations.*

Design and Methodology

To test our hypotheses, we used a novel application of the factorial survey method (Jasso 2006; Rossi 1979; Wallander 2009), a variation of the scenario method often used to study ISP violations. The respondents consisted of employees with administrative access to the academic records system (ARS) of a large private university. We chose this sample frame and organizational context because the ARS, in terms of both scope and risk of potential abuse, is characteristic of unauthorized access problems similar to a variety of sectors.[4] Notably, access-policy violations within the university's ARS are also violations of the Family Educational Rights and

[4]Our sample frame was chosen because ARS shares many of the features and risks described previously, including the following:

(1) **Sensitive information**: ARS contains personally identifiable information belonging to current and former members of the university, including students and alumni, applicants, and employees.

(2) **Scope**: The ARS comprises terabytes of data corresponding to approximately 1.54 million individuals, going back to 1969, when the first computerized records were brought online at the university.

(3) **Broad-access privileges**: Employee users of the ARS are given broad-access privileges in the system so they can assist any current or former student, regardless of academic discipline.

(4) **Legal compliance**: Student records in the U.S. are protected by FERPA, enacted in 1974. Violations of FERPA may include the withdrawal of federal funding from the educational institution. Consequently, FERPA compliance is a key control and governance focus at U.S. universities.

(5) **Access policy**: The university has clear policies directing the appropriate use of access privileges within the ARS. All employee users of the ARS must complete the university's FERPA training before gaining access to the system. Additionally, a compliance officer oversees FERPA compliance across the university and holds regular refresher training sessions on appropriate access.

(7) **Potential for unauthorized access abuse**: Like other systems of this nature, ARS has been subject to university-documented instances of FERPA violations due to unauthorized access, some of which have been very costly to resolve and detrimental to public relations. Although documented violations are relatively uncommon, they are nonetheless distressing for the university.

In summary, the university ARS is vulnerable to abuse from unauthorized access problems that are similar, in terms of both scope and risk, to those that can affect the systems used in a variety of business sectors, including health care, finance, and government.

Privacy Act (FERPA), a U.S. law that protects student privacy at U.S. universities.

The Scenario Method Versus the Factorial Survey Method

The *factorial survey method* is a specialized form of the *scenario method* (a.k.a., vignette method), which uses vignettes that "present subjects with written descriptions of realistic situations and then request responses on a number of rating scales that measure the dependent variables of interest" (Trevino 1992, pp. 127-128). The scenario method is useful for studying unauthorized access violations for several reasons. First, scenarios can incorporate situational details considered important in decisions to behave unethically (Klepper and Nagin 1989). Because "the situational context of decision making and the information being handled will vary greatly among offenses" (Clarke and Felson 1993, p. 6), scenarios can enhance the realism of decision-making situations by providing contextual detail while simultaneously ensuring the uniformity of these details across respondents (Alexander and Becker 1978).

Second, scenarios afford an indirect way of measuring the intention to commit unethical behavior, which is difficult to measure directly (Trevino 1992). Because scenarios describe another's behavior in hypothetical terms, the respondent might feel less concerned about reporting an intention to act similarly to the person in the scenario (Harrington 1996). For these reasons, the scenario method is the one most commonly applied for studying ethical issues (O'Fallon and Butterfield 2005) and is thus increasingly used to study computer abuse and IS policy violations (e.g., D'Arcy et al. 2009; Hu et al. 2011; Siponen and Vance 2010).

Pioneered by Rossi and his colleagues (Rossi 1979; Rossi and Anderson 1982; Rossi et al. 1974) and applied in well over 100 sociological studies (Wallander 2009), the *factorial survey method* has been called the methodological "gold standard" for accessing ethical beliefs and normative judgments (Seron et al. 2006, p. 931). The purpose of the factorial survey method is to "uncover the social and individual structures of human judgments of social objects" (Wallander 2009, p. 505).

The factorial survey method differs from typical scenario-based surveys in that textual (and in our unique application, graphical) elements within the scenario are experimentally varied. This technique combines the rich number of factors afforded by field survey methods with the control and orthogonality provided by experimental designs (Rossi 1979). It has also proved useful for explaining white-collar crime (Paternoster and Simpson 1996), a context very similar to ISP violations such as unauthorized access.

Notably, the factorial survey is *neither* an experiment *nor* a traditional survey, but draws on both to provide a truly unique method. Similar to experiments, factorial surveys are constructed by designing *dimensions* or factors of theoretical interest. In turn, each dimension comprises several levels, which are analogous to treatments within an experimental factor. These dimensions and levels are then textually incorporated into the vignettes. The method is called a *factorial survey* because a full factorial of all possible combinations of levels and dimensions is obtained, forming a Cartesian product. The full factorial ensures that the levels are orthogonal, with correlations at or near zero, thus overcoming the problem of multicollinearity (Jasso 2006). Orthogonality allows us to distinguish clearly between the different effects of our UI design artifact manipulations. Using a traditional survey would have made it difficult or impossible to eliminate multicollinearity between our manipulations (Rossi and Anderson 1982).

Like traditional surveys, factorial surveys adopt the technique of statistical random sampling. From the population of the full factorial, a random sample of vignettes (called a *pack*) is obtained, which typically contains between 10 and 60 vignettes (Jasso 2006). Each survey respondent receives his/her own pack and gives a response (e.g., reports a level of intention) for each vignette contained in the pack. Estimates of dimensions in the full factorial population are made from the sample of responses to the vignettes received in the pack. In this way, estimates for a wide variety of factors can be obtained. Traditional experimental designs are limited to supporting a factorial of only a few dimensions with a few levels each before becoming impractically complex (Rossi and Anderson 1982). Factorial surveys do not share this limitation. Because random sampling is used, many factors and levels can be used to create a factorial of hundreds, thousands, or even millions of unique vignette combinations (Jasso 2006). This provides a rich set of factors that more closely approximates the real world, and we propose as ideal for evidence-based design science of IT artifacts.

Scenario Design

To create our factorial survey, we first consulted with the university FERPA compliance officer to jointly create eight instructional scenarios that described common access requests that would be policy violations for the university. These scenarios provided the contextual foundation upon which the

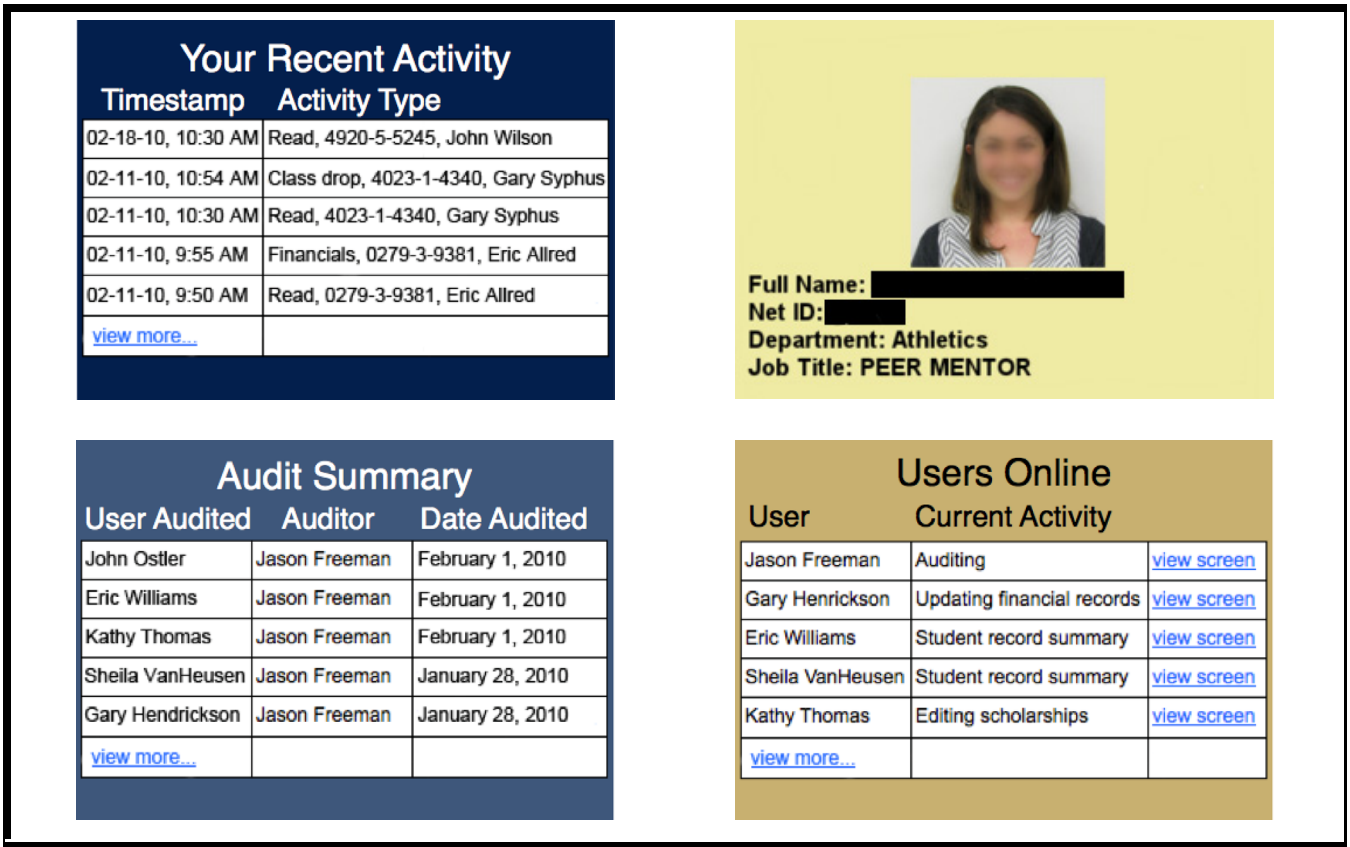

Figure 2. UI Design Artifacts of the Graphical Vignettes

respondents considered the UI design artifacts contained in the graphical vignettes. Unlike scenarios in traditional factorial surveys, the scenarios themselves did not contain embedded independent variables. Rather, such variables were embedded in the graphical vignettes. Also, the respondents did not complete measures of the dependent variables after receiving the scenarios. Instead, dependent variables were captured only after respondents viewed each graphical vignette.

Per Siponen and Vance (2014), the scenarios were validated for contextual validity and realism by eliciting feedback from four employee users with broad-access privileges within ARS.

All eight scenarios are reproduced in Appendix B. Half of the eight scenarios are virtual duplicates of the other half, the difference being that half explicitly mention that the scenario character believes that the behavior in question would constitute a violation of university policy, whereas the other half make no mention of university policy. This variation allowed us to examine both the effect of the respondents' knowledge that an access-policy violation was involved and whether such knowledge introduced a social desirability bias.

Graphical Design of the Factorial Survey

We developed four graphical UI design artifacts corresponding to the effects of (1) identifiability, (2) expectation of evaluation, (3) awareness of monitoring, and (4) social presence. Figure 2 depicts these artifacts, which constitute our only independent variables. The design science implications for these artifacts are discussed in Appendix C. The UI design artifacts were consistent across respondents, except for the identifiability artifact, which displayed a respondent's personal employment ID photo. Our sample frame consisted of all employee users of the ARS, and we obtained photos and employee information for each sample member. We created a unique identifiability UI design artifact that displayed each respondent's actual photo, name, employee identifier, job title, and department. In addition to increasing the realism of and personal connection to the factorial survey, this design helped to heighten the respondent's perception of being identified in the ARS. Each of the four UI design artifacts had two levels: visible and not visible. These artifacts combined to create a factorial of 16 unique graphical vignettes ($2 \times 2 \times 2 \times 2$). Each graphical vignette was then superimposed over a screenshot of the ARS login screen. To help respondents

Figure 3. A Sample Graphical Vignette (One of Four Received by this Respondent)

distinguish between the screenshots, labels were added to emphasize the presence or absence of each UI design artifact (see Figure 3).

Each respondent received 4 of the 16 possible combinations of graphical vignettes randomly. To help respondents distinguish between the UI design artifacts, one of four background colors was assigned randomly as the background. To reduce positioning bias, we randomly varied the position occupied by the UI design artifact in the screenshot.

Survey Instrument

The factorial survey instrument involved pre-scenario items, an instructional scenario, post-scenario items, graphical vignettes, and post-vignette items. Figure 4 depicts the timeline sequence of these elements. First, the respondent answered demographic questions regarding gender, age, employment status, and level of education obtained. Second, the respondent answered questions about the degree to which he/she felt accountable for his/her actions in the current ARS. Third, the respondent read one of the eight instructional scenarios describing an unauthorized access violation. Fourth, the respondent gauged the perceived wrongness of the violation using a moral intensity scale. Fifth, the respondent was presented with the instructional scenario again, this time along with one of the four graphical vignettes.

As part of this fifth step, the respondent had the opportunity to report his/her intention to act as the character did, given the context provided in the instructional scenario and the UI design artifacts depicted in the graphical vignette. The accountability scale was then administered again—this time asking how accountable the respondent would feel if the ARS featured UI design artifacts like those depicted in the graphical vignette. This fifth step was repeated for each of the four graphical vignettes received.

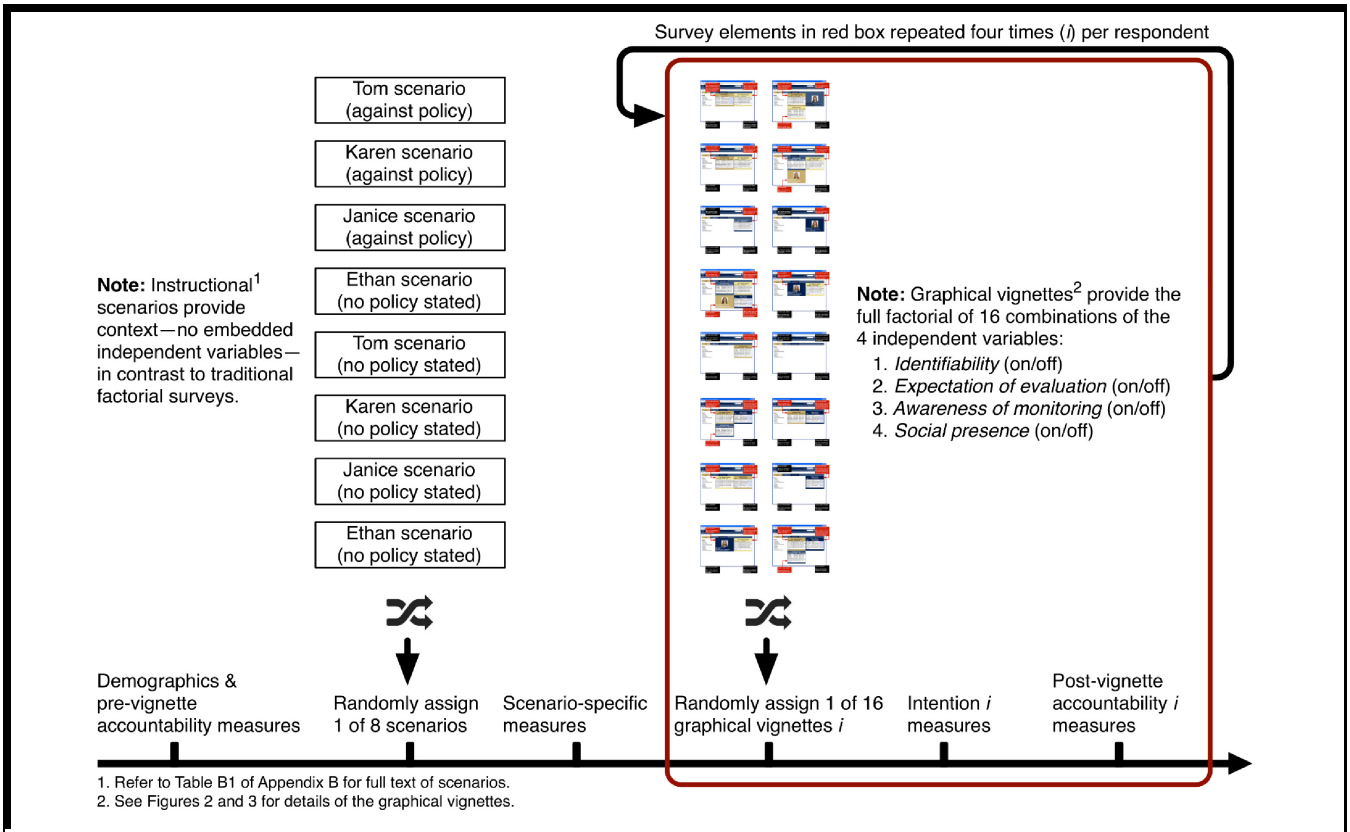

Figure 4. Sequence of Items, Instructional Scenarios, and Vignettes in the Factorial Survey Instrument

Data Collection

We first conducted a pilot test.[5] The final sample frame was drawn randomly from the set of all ARS users. This amounted to a sample frame of 1,190 users. Of these, we received 318 completed surveys, resulting in a response rate of 27 percent. As is typical with factorial survey designs, the level of analysis was not the participant, but the vignette (Jasso 2006). Thus, because each respondent rated four graphical vignettes, the final N for the survey was 1,272.

Analysis and Results

The dependent variable for the analysis was the participant's reported intention to violate the access policy just as the scenario character did, given the UI design artifacts depicted in the graphical vignette. The four UI design artifacts depicted in Figure 2 served as the predictors and were analyzed as categorical variables. Because each respondent rated multiple graphical vignettes, the observations were not independent. Unobserved differences (i.e., heterogeneity) in the respondents constituted a fixed individual effect that biased the vignette ratings for each respondent (Greene 2011). Because ordinary least squares (OLS) analysis does not handle mixed models of fixed and random effects, another approach to analysis was necessary (Piquero et al. 2005). To control for the individual effect, we selected the SAS PROC MIXED procedure, a generalized form of the standard linear model that allows for both fixed and random effects (McLean et al. 1991).[6]

[5]We pilot tested the instrument and factorial survey design using a random sample of 114 employees from the set of ARS administrative users. This sample of ARS users was separate from those of the primary data collection. Because the survey used a repeated measures design in which each user responded to four vignettes, the N for the pilot test was 456. Based on feedback on the pilot test, the instrument was further clarified and refined. Reliabilities of the survey items were calculated, and items were modified or dropped from the instrument as needed.

[6]In contrast to OLS, the PROC MIXED procedure uses maximum likelihood estimations, as do covariance-based structural equation modeling techniques (Gefen et al. 2000). The variance estimates adjust for the correlation that

Control Variables and Rival Predictors

We collected data for the demographic variables to use as control variables as well as for psychometric measures to use as rival predictors. The items and sources for these rival predictors are described in Appendix B. Validation for the instrumentation is reported in Appendix D. Appendix E describes the testing of the variables and their selection in a baseline model.

Theoretical Model Test

In our model (Figure 1), we were not interested in the effect of perceived accountability alone, but rather the effect of the increase in perceived accountability from the pretest measurement to the posttest, as induced by the UI design artifacts. Thus, we first discuss the testing of our main effects model, then the mediation portion of the model.

Testing the Main Effects Model

First, we tested hypotheses 1–4. To do this, we first calculated the effect of the *change of perceived accountability* (hereafter *Δaccountability*) as the difference between the posttest and pretest scores for perceived accountability. We then specified a model that incorporated the change in accountability as the dependent variable and the UI design artifacts as independent variables. Table 1 summarizes the results of this test. All four UI design artifacts were significant, supporting H3–H6, with substantial effects.[7]

To determine whether the UI design artifacts collectively increased accountability within the ARS (H5), we used pre-vignette and post-vignette accountability measures. If the accountability mechanisms depicted in the vignette influence perceived accountability, then the post-vignette accountability measures should be higher than pre-vignette measures. We calculated the difference in perceived accountability between the posttest and the pretest and entered this result into a model with no predictors. The intercept of this model was 1.58, indicating that the posttest score for perceived accountability was on average 1.58 higher (on a scale of 1 to 7) than the pretest score, representing a 26.3 percent increase (t-value 3.21; $p < .002$). Hence, we conclude that the UI design artifacts did increase accountability. This confirms that the manipulations were received effectively by the users and, importantly, that UI design artifacts can indeed directly increase accountability in general (H5 supported).

We then examined the effect of *Δaccountability* on *intention to violate the access policy*. Table 2 summarizes these results. As predicted, *Δaccountability* strongly reduced *intention to violate the access policy* (-.187; $p < .001$), supporting H6**.** The fit scores for the theoretical model were also substantially improved, with Akaike's information criterion (AIC) and Schwarz's Bayesian information criterion (BIC) significantly lower than those of the control model ($p < .001$).[8] The test for significant difference between models in terms of either AIC or BIC is a likelihood ratio test. The test statistic is distributed as a chi-square distribution, and p-values are calculated using the statistic relative to its degrees of freedom (Littel et al. 1996). Therefore, we conclude that adding *Δaccountability* to the model explains *intention to violate the access policy* substantially better than do the rival predictors alone, and with a very large effect size.[9]

Testing for Mediation in the Model Using Bootstrapping Analysis

We hypothesized that *Δaccountability* would mediate the effects of each of the UI design elements (H7a–d). To test these

exists in our data. That correlation comes from the repeated measures (i.e., each participant rated four graphical vignettes). Thus, each participant's four ratings are correlated with one another—constituting a fixed individual effect (Paternoster and Simpson 1996). Typical least-squares analysis does not account for such correlation, rendering incorrect the variance estimates used for the statistical tests. Conversely, the maximum likelihood estimates from PROC MIXED are accurate estimates, accounting for the correlation in the data (Littel et al. 1996).

[7]To understand the size of these effects, we evaluated the coefficients for each of the UI design artifacts. Because the UI design artifacts were measured as dummy variables (0 for not present; 1 for present), the coefficients for the variables in Table 3 represent the average increase in Δaccountability. Thus, the identifiability treatment increased Δaccountability by .793, the evaluation-logging treatment increased Δaccountability by 1.21, and so forth. Because the post-accountability sum variable had a range of 18 (3 to 21), the treatments resulted in a 4.4% to 6.7% increase in accountability, representing relatively small, although significant, effects. However, the sum of the effects for all UI design artifacts resulted in a 19% change in accountability (3.44/18), a substantial effect.

[8]Both AIC and BIC are functions of the log likelihood for a given model. Moreover, both statistics penalize a model for including terms that do not contribute substantially to the fit of the model. The statistics differ in the size with respect to the penalty size. For both statistics, a lower value indicates a better-fitting model with fewer unnecessary terms. Therefore, the goal is to minimize either the AIC or BIC when comparing rival models (Ramsey and Schafer 2013).

[9]The size of the effect of *Δaccountability* can be understood in terms of the scale of the dependent variable, the range of the difference of the change in accountability, and the parameter estimate (-.187) in the model. For every unit increase in *Δaccountability*, intention was reduced by -.187. Because the values for the change in accountability had a range of 32, intention could be reduced by up to -5.76 (-.187 · 32). Because intention was measured on a 0 to 10 scale, this represents a very large effect size.

Table 1. Effects of UI Design Artifacts on the Change in Perceived Accountability

Effect	β	Standard Error	*t*-Value
Intercept	.235	1.369	.17 n.s.
Subjective norms	.118	.078	1.51 n.s.
Education level	.094	.117	.80 n.s.
Scenario 1	-.011	.518	.02 n.s.
Scenario 2	.251	.525	.48 n.s.
Scenario 3	.491	.521	.94 n.s.
Scenario 4	0	0	0
Moral intensity	.024	.051	.48 n.s.
Identifiability	.793	.134	5.90***
Expectation of evaluation	1.120	.152	7.38***
Awareness of monitoring	1.207	.130	9.29***
Social presence	.324	.129	2.52*

Fit statistics: AIC = 6205.3; BIC = 6212.8; Degrees of freedom: intercept = 311; all others = 950

***p < .001; **p < .01; *p < .05; n.s. = not significant

Table 2. Effects of *Δaccountability* on Intention to Violate the Access Policy

Effect	β	Standard Error	*t*-Value
Intercept	6.479	1.333	4.86***
Subjective norms	-.549	.077	7.17***
Education level	-.332	.115	2.90**
Scenario 1	.055	.507	1.1 n.s.
Scenario 2	-.060	.514	1.2 n.s.
Scenario 3	1.303	.510	2.55*
Scenario 4	0	0	0
Moral intensity	.246	.050	4.94***
Δaccountability	-.187	.017	11.16***

Fit statistics: AIC = 5254.6; BIC = 5262.1; degrees of freedom: intercept = 311; all others = 953

***p < .001; **p < .01; *p < .05; n.s. = not significant

hypotheses, we used bootstrapping to construct confidence intervals (CIs) of the mediation effects. Whereas the Baron and Kenny (1986) method and the Sobel (1982) method have traditionally been used to test for mediation effects, advances in computing power have enabled more accurate and powerful statistical mediation testing through bootstrapping (Shrout and Bolger 2002). In addition to greater statistical power, an advantage of the bootstrapping approach is that indirect effects can be measured directly rather than merely inferred to exist through a sequence of tests, as seen in the Baron and Kenny method (Hayes 2009). Another advantage of bootstrapping is that it does not assume that the mediation effect is normally distributed, as does the Sobel method. This is important, because studies have shown that indirect effects frequently exhibit asymmetric distributions. In such cases, using a test that assumes a normal distribution results in lower statistical power (MacKinnon et al. 2002).

Testing mediation effects with bootstrapping is similar to the Baron and Kenny method in that three paths are evaluated: (1) the path from the independent variable to the mediating variable (path a), (2) the path from the mediating variable to the dependent variable (path b), and (3) the path from the independent variable to the dependent variable (path c, or c' when considered simultaneously with paths a and b).

The bootstrapping process involves resampling with a replacement from the obtained sample several thousand times. For each resample, the coefficient of path a is multiplied by the coefficient of path b. The product of ab is the estimate of

Table 3. Bootstrapped CI Tests for Full and Partial Mediation

	Mediation Test (*ab*)			Full/Partial Mediation Test (*c′*)			
Variable	2.5% lower bound	97.5% upper bound	Zero included?	2.5% lower bound	97.5% upper bound	Zero included?	Type of mediation
Identifiability	.089	.220	No	-.022	.252	Yes	Partial
Awareness of monitoring	.133	.320	No	.108	.513	No	Full
Expectation of evaluation	.146	.333	No	.059	.377	No	Full
Awareness of social presence	.002	.142	No	.035	.366	No	Full

the indirect effect in the resample (MacKinnon et al. 2002). The coefficient for c' is also saved. The process is repeated k times, where k is a number equal to at least 1,000 and preferably equal to or greater than 5,000 (Hayes 2009). At the end of the bootstrapping process, thousands of values for ab and c' are obtained.

Next, the values for ab and c' are sorted from largest to smallest and a percentile-based CI is constructed (ci%). This is done by identifying the ordinal positions of ab and c' that correspond to the bounds of the CI, using the formula $k(.5 - ci/200)$ for the lower bound and the formula $1 + k(.5 + ci/200)$ for the upper bound (Hayes 2009). In our case, we obtained 5,000 resamples and specified a 95% CI. For the sorted ab values, the lower bound of the CI was represented by the ab value in the 125th position.

For the ab CI, if zero is not between the lower and upper bound, then one can state with ci% confidence that the indirect effect is not zero (MacKinnon 2008). It is possible to determine whether full or partial mediation occurred by examining the CI for c'. If ab is nonzero and c' is zero, this result indicates full mediation. If both ab and c' are nonzero, then this result is evidence of partial mediation (Shrout and Bolger 2002).

We followed the above procedures to bootstrap the effects of our four graphical UI elements on *Δaccountability* (paths a_{1-4}) using PROC MIXED and a macro to obtain 5,000 resamples. We did the same for the effect of *Δaccountability* on intention to violate the access policy (path b) and for the effects of our four graphical UI elements on intention (c'_{1-4}). Table 3 reports the 95 percent CIs for each path; whether zero was obtained in the CI, indicating mediation; and whether full or partial mediation was observed.

The results show that the effect of each of the graphical UI elements was mediated by *Δaccountability*, with identifiability being mediated partially, and awareness of monitoring, expectation of evaluation, and awareness of social presence being mediated fully. This result indicates that whereas the effects of awareness of monitoring, expectation of evaluation, and awareness of social presence on intention are explained wholly by *Δaccountability*; identifiability has a direct negative effect on intention beyond that which is mediated by *Δaccountability*. Identifiability may therefore have a psychological effect apart from simply increasing accountability. Together, our results support H7a–d, which hypothesized that *Δaccountability* would mediate the effects of the UI design artifacts. In addition, we conducted a series of exploratory *post hoc* tests that showed significant interactions (see Appendix F). Table 4 summarizes the results of our hypothesis testing. Finally, we performed tests to demonstrate that our research did not suffer from social desirability bias (see Appendix G).

Discussion

Access-policy violations in organizations are a growing problem. Technical means of securing systems have limited power to mitigate this problem, because many systems in business, government, and health care require broad-access privileges and do little to deter the abuse of legitimate system privileges. Hence, it is imperative to identify additional ways to thwart access-policy violations. This paper makes four principal contributions to this endeavor.

UI Design Artifacts

Our first research question asked how UI artifacts can be designed to increase accountability in users of a broad-access system. We developed UI design artifacts for an actual system used frequently by of all our research participants. We then empirically tested these artifacts with the employees who had privileged access within that system. Scholars have criticized IS research for the frequent absence of the IT artifact; our contribution, however, is both theoretical and artifactual (Gregor and Hevner 2013; Hevner et al. 2004). Our results extend those of Vance et al. (2013)—who used textual scenarios without an instantiated IT design artifact—to support the

Table 4. Summary of Hypothesis Testing

Hypothesis	Supported?	Type of Effect
H1. UI artifacts that manipulate identifiability will increase accountability.	Yes	Direct effect
H2. UI artifacts that manipulate expectation of evaluation will increase accountability.	Yes	Direct effect
H3. UI artifacts that manipulate awareness of monitoring will increase accountability.	Yes	Direct effect
H4. UI artifacts that manipulate social presence will increase accountability.	Yes	Direct effect
H5. Collectively, UI artifacts that manipulate accountability mechanisms will increase accountability.	Yes	Direct effect
H6. Perceived accountability decreases intention to commit access-policie violations.	Yes	Direct effect
H7. Accountability will mediate the effects of user-interface artifacts for (1) identifiability, (2) expectation of evaluation, (3) awareness of monitoring, and (4) social presence on the intention to commit access-policy violations.	(1) Yes	Partial mediation
	(2) Yes	Full mediation
	(3) Yes	Full mediation
	(4) Yes	Full mediation

idea that manipulations of the UI can be effective in reducing unauthorized access violations. The distinction between the hypothetical manipulations of Vance et al. (2013) and the realized UI design artifacts of this paper can be understood through the pivotal design science concepts of *proof-of-concept* and *proof-of-value*. We elaborate on these distinctions and our contributions to design science in Appendix C.

The difference between typical deterrence approaches and the accountability UI approach we put forward highlights the contributions of our UI design artifacts in the context of access-policy violations. Deterrence applications call for employees to be warned, threatened, trained, and reminded about sanctions over a certain period of time. The implementation of deterrence programs can be not only coercive and time consuming, but also disruptive, because deterrence activities function outside of employees' normal course of business. Thus, such approaches have been known to backfire and create negative, unintended consequences for organizations.

Our study turns the tables by eliciting compliant behavioral intentions through accountability mechanisms embedded in the UI. Our UI design features are minimally intrusive and do not rely on heavy-handed approaches based on DT. Without overt warnings, training, threats, or sanctions, our UI design artifacts caused strong cognitive changes through the construct of accountability in seconds. Importantly, our manipulations occurred on a subtle cognitive basis while employees were engaged in their normal work tasks. Thus, our approach is less disruptive than conventional deterrence approaches and can be integrated more seamlessly into the realities and pressures of employees' day-to-day work. Just as important, our approach can persuade employees to engage in protection-motivated behaviors toward organizational systems, as has been called for in recent research (e.g., Posey et al. 2013; Posey et al. 2014).

The managerial implications of this study are exciting and, again, offer alternatives to heavy-handed approaches. First, rather than requiring explanations and training that take hours or days, our interventions involve no formal education and can elicit positive intentions in seconds. Second, being based in design principles, our UI design artifacts can potentially be implemented in virtually any kind of system. Third, our UI design artifacts work to reinforce each other through interactions; thus, multiple UI design artifacts implemented in a system are better than one. Fourth, there is also the potential for other UI design artifacts to be developed, pointing to future theoretical and design science research opportunities.

Influence of Accountability on Access-Policy Violation Intentions

Our second research question asked whether accountability could effectively reduce intentions to violate access policies. We showed that perceived accountability strongly predicted the intention to violate the access policy with a very large effect size, over and above our rival predictors and control variables (e.g., subjective norms, education, instructional scenario received, and moral intensity). We thus conclude that accountability is an effective means of reducing access-policy violations.

This finding shows that accountability is a useful mechanism for reducing intentions to violate access policies. Moreover, our results suggest that accountability may reduce other forms of ISP violation as well as general computer abuse. In such cases, accountability shows promise as an alternative, less

heavy-handed means of reducing nonconforming behaviors. Whereas the heart of DT is a cost-benefit analysis of a given violation, the central mechanism of accountability is self-image preservation and social approval. This suggests that accountability mechanisms may serve as a viable alternative—or supplement—to sanctions.

Mediation Effect of Perceived Accountability

Our third research question asked whether perceived accountability mediates the effects of the UI design artifacts on the intention to violate access policies. This question is crucial because we need to determine whether the UI design artifacts influence violation intentions through the operation of the construct of perceived accountability, whether they do so through some theoretical construct, or whether they simply influence intentions directly.[10] We theorized on why accountability mediates the individual effects of the UI design artifacts on the intention to violate the access policy.

Using robust bootstrapping tests for mediation, we were also able to establish that perceived accountability significantly mediates the effects of all four UI design artifacts. We found that perceived accountability fully mediated the effects of expectation of evaluation, awareness of monitoring, and social presence. In contrast, the effect of identifiability was partially mediated, indicating that it has a direct effect on the intention to violate access policy apart from its influence on intention through accountability. This mediation analysis further validates the role of accountability as the key mechanism fostered by our UI design artifact manipulations.

Here, we point out the theoretical and empirical importance of the first study to establish accountability as a mediator. As Whetten (1989) states, "Relationships, not lists, are the domain of theory" (pp. 492-493) and "theoretical insights come from demonstrating how the addition of a new variable significantly alters our understanding of the phenomena by reorganizing our causal maps" (p. 493). The general weakness of adding independent variables (IVs) is that these are often done to complete "lists," often have little theoretical basis, and are typically added in an exploratory manner (Whetten 1989). Thus, establishing moderation or mediation is much more interesting theoretically; doing so demonstrates a fundamental change in relationships (Muller et al. 2005). Of the two, mediation represents the larger theoretical contribution, because it profoundly changes the extant literature's current explanation narrative (Whetten 2009). Because we have established basic mediation (x → z → y), there are now two IVs and DVs where there used to be only one of each, and a sense of process and causal mechanisms has been introduced (Muller et al. 2005).

Methodological Contributions

We also provide several methodological contributions that can improve design science and behavioral research. First, we illustrated a novel application of the scenario-based factorial survey method by presenting graphical vignettes of the UI design artifacts to respondents—as opposed to the usual practice of purely textual scenarios, which has been widely followed in the recent past (e.g., Lowry et al. 2013; Vance et al. 2013). This technique is particularly exciting because it can be leveraged in many research contexts to more quickly and more powerfully evaluate the effects of multiple design artifacts on real end users without extreme sampling requirements. This new approach goes beyond traditional laboratory experiments and HCI research in which so many UI design combinations simply cannot be studied in one setting.

Second, by using bootstrapping, we demonstrated an advanced technique of testing for mediation and moderation in factorial survey data that is more powerful than traditional techniques. Aside from greater statistical power, another advantage of the bootstrapping approach is that it can measure indirect effects directly instead of merely inferring that they exist through a sequence of tests, as in the Baron and Kenny method. Another advantage of bootstrapping is that it does not assume that the mediation effect is normally distributed, which is often not the case. Our analysis approach can thus be leveraged to test mediation, mediated moderation, and moderated mediation more effectively than current practices in IS research.

Third, we validated our model using working professionals who had broad-access privileges in the ARS, embedding their personal information and photos in the UI design artifacts of the factorial survey. Likewise, following the best research practice of engaging with the context of practitioners, we worked directly with the university's FERPA compliance officer to develop scenarios that describe common and realistic access requests that would be highly problematic violations. Our field research setting, which built on an actual ARS used by thousands of employees, increased the likelihood that the results are relevant to practice. The sensitive ARS contained many terabytes of data that involved the following key characteristics: sensitive information, broad-access privileges to hundreds of employees, required government legal compliance, established access policies, and high potential for access-policy violations.

[10]Regarding this research question, Vance et al. (2013) implied that this mediating relationship exists, but they did not theorize on why this effect should occur and did not empirically test for mediation.

Limitations and Future Research

This study has several limitations that point to promising research opportunities. First, although support for four different accountability design artifacts was found, other design features, such as reason giving, may increase accountability perceptions among users and deter unauthorized access. Further research is needed to identify other relevant accountability submanipulations that can be usefully implemented as UI design artifacts.

Research could also expand the foundation of accountability theory itself. Accountability theory leverages the core cognitive psychology concept of systematic processing as a causal mechanism that helps create accountability. Complementing the idea of systematic processing is the idea of heuristic or superficial processing. Heuristic processing has never been addressed by accountability theory, but it could provide an interesting extension. Several dual-processing models have been proposed in cognitive psychology, such as the elaboration likelihood model and the heuristic–systematic model. Finding ways to measure and thwart superficial or heuristic processing in accountability creation could be a fruitful future research endeavor.

We also examined intentions using graphical vignettes rather than actual behavior within a real system, which is the established best practice. Nonetheless, although it is difficult to discover and measure computer abuses directly in actual work settings—as is also the case with other forms of socially undesirable behavior—a qualitative field study of an actual system in use could provide additional insights to further test our model in practice. An alternative approach would incorporate observation of actual access-policy violations over time and compare a system and its users before and after UI design artifacts were introduced to increase accountability.

Another limitation is that we did not examine boundary conditions for the effects of accountability within systems. Because some research has pointed to the negative effects of monitoring conducted in a heavy-handed manner, more accountability may not always be better. Breaux et al. (2008) found that accountability had negative effects under conditions of supervisory abuse. Thus, an avenue for future research is to determine under what conditions accountability is beneficial for users' compliance with ISPs and when it may become detrimental.

Another limitation is that our study was solely in a Western context in terms of users and underlying laws (i.e., FERPA). Yet, research has shown that culture plays an important role in determining outcomes in systems use (Lowry, Zhang et al. 2010; Posey et al. 2010; Vance et al. 2008). Moreover, recent research has shown key cultural differences in determining actual employee computer abuse (Lowry, Posey et al. 2014). Hence, cultural considerations should be included in future expansions of accountability theory.

Finally, the next task for future research on UI design artifacts and accountability is to directly compare the effectiveness of sanctions suggested by DT and accountability mechanisms, such as those we examined. Such research could examine whether accountability mechanisms can effectively replace heavy-handed sanctions or whether deterrence and accountability mechanisms are complementary and should be used in a balanced fashion. Additionally, whereas deterrence mechanisms are designed solely to dissuade antisocial behaviors, accountability mechanisms can also foster prosocial behaviors (see Appendix A). Future research should examine whether the UI design artifacts are also effective in encouraging prosocial behaviors, as accountability theory predicts. For example, researchers could examine whether accountability mechanisms are effective in encouraging behaviors beneficial to security, such as backing up data, keeping software up to date, and taking optional SETA training.

Conclusion

We demonstrated the potential for theory-based UI artifact manipulations to increase accountability in employees—and thereby decrease intentions to violate organizational access policy. We tested our model using a novel application of the factorial survey method, with professional users of a system vulnerable to committing access-policy violations. The results demonstrated that our UI artifacts substantially increase accountability and reduce intentions to commit access-policy violations in systems. We conclude that accountability UI artifacts are a promising, novel solution that supplements the efforts of traditional security mechanisms to reduce access-policy violations in a nonintrusive manner.

References

Alexander, C. S., and Becker, H. J. 1978. "The Use of Vignettes in Survey Research," *Public Opinion Quarterly* (42:1), pp. 93-104.

Argelaguet, F., Kulik, A., Kunert, A., Andujar, C., and Froehlich, B. 2011. "See-Through Techniques for Referential Awareness in Collaborative Virtual Reality," *International Journal of Human–Computer Studies* (69:6), pp. 387-400.

Baron, R. M., and 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), pp. 1173-1182.

Baumeister, R. 1982. "A Self-Presentational View of Social Phenomena," *Psychological Bulletin* (91:1982), pp. 3-26.

Bond, C., and Titus, L. 1983. "Social Facilitation: A Meta-Analysis of 241 Studies," *Psychological Bulletin* (94:1983), pp. 265-292.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

Bovens, M. 2010. "Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism," *West European Politics* (33:5), pp. 946-967.

Breaux, D., Perrewe, P., Hall, A. T., Frink, D., and Hochwarter, W. A. 2008. "Time to Try a Little Tenderness? The Detrimental Effects of Accountability When Coupled with Supervision," *Journal of Leadership and Organizational Studies* (45:1), pp. 80-83.

Burton-Jones, A., and Hubona, G. S. 2006. "The Mediation of External Variables in the Technology Acceptance Model," *Information & Management* (43:6), pp. 706-717.

Chaiken, S., and Maheswaran, D. 1994. "Heuristic Processing Can Bias Systematic Processing Effects of Source Credibility, Argument Ambiguity, and Task Importance on Attitude Judgment," *Journal of Personality & Social Psychology* (66:3), pp. 460-473.

Clarke, R., and Felson, M. 1993. "Criminology, Routine Activity and Rational Choice," in *Routine Activity and Rational Choice,* R. Clarke, and M. Felson (eds.), New Brunswick, NJ: Transaction Publishers, pp. 1-14.

Cottrell, N. B. 1972. "Social Facilitation," in *Experimental Social Psychology,* C. McClintock (ed.), New York: Holt, Rinehart & Winston, pp. 185-236.

Crano, W. D., and Prislin, R. 2006. "Attitudes and Persuasion," *Annual Review of Psychology* (57:1), pp. 345-374.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:1), pp. 90-101.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Deml, B. 2007. "Human Factors Issues in the Design of Telepresence Systems," *Presence: Teleoperators and Virtual Environments* (16:5), pp. 471-487.

Diener, E., Fraser, S., Beaman, A., and Kelem, R. 1976. "Effects of Deindividuation Variables on Stealing among Halloween Trick-or-Treaters," *Journal of Personality and Social Psychology* (33:1976), pp. 178-183.

Fandt, P., and Ferris, G. 1990. "The Management of Information and Impressions: When Employees Behave Opportunistically," *Organizational Behavior and Human Decision Processes* (45:1990), pp. 140-158.

Galletta, D. F., and Hufnagel, E. M. 1992. "A Model of End-User Computing Policy: Context, Process, Content and Compliance," *Information & Management* (22:1), pp. 1-18.

Geen, R. 1991. "Social Motivation," *Annual Review of Psychology* (42:1991), pp. 377-399.

Gefen, D., Straub, D. W., and Boudreau, M. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4:7), pp. 1-30.

Greene, W. 2011. *Econometric Analysis*, Upper Saddle River, NJ: Prentice Hall.

Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly* (37:2), pp. 337-355.

Griffith, T. 1993. "Monitoring and Performance: A Comparison of Computer and Supervisor Monitoring," *Journal of Applied Social Psychology* (23:1993), pp. 549-572.

Guerin, B. 1986. "Mere Presence Effects in Humans: A Review," *Journal of Experimental Social Psychology* (22:1986), pp. 38-77.

Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257-278.

Hayes, A. F. 2009. "Beyond Baron and Kenny: Statistical Mediation Analysis in the New Millennium," *Communication Monographs* (76:4), pp. 408-420.

Herath, T., and Rao, H. R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75-105.

Hochwarter, W., Ferris, G., Gavin, M., Perrewé, P., Hall, A., and Frink, D. 2007. "Political Skill as Neutralizer of Felt Accountability: Job Tension Effects on Job Performance Ratings: A Longitudinal Investigation," *Organizational Behavior and Human Decision Processes* (102:2), pp. 226-239.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp. 54-60.

Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research* (34:3), pp. 334-423.

Johnson, M. E., and Willey, N. D. 2011. "Usability Failures and Healthcare Data Hemorrhages," *IEEE Security & Privacy* (9:2), pp. 35-42.

Kahai, S. S. 2009. "Anonymity and Counter-Normative Arguments in Computer-Mediated Discussions," *Group Organization Management* (34:4), pp. 449-478.

Karat, J., Karat, C. M., Brodie, C., and Feng, J. J. 2005. "Privacy in Information Technology: Designing to Enable Privacy Policy Management in Organizations," *International Journal of Human–Computer Studies* (63:1-2), pp. 153-174.

Kenny, D. A. 2008. "Reflections on Mediation," *Organizational Research Methods* (11:2), pp. 353-358.

Klepper, S., and Nagin, D. 1989. "The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited," *Criminology* (27:4), pp. 721-746.

Kock, N. 2004. "The Psychobiological Model: Towards a New Theory of Computer-Mediated Communication Based on Darwinian Evolution," *Organization Science* (15:3), pp. 327-348.

Lerner, J. S., and Tetlock, P. E. 1999. "Accounting for the Effects of Accountability," *Psychological Bulletin* (125:2), pp. 255-275.

Littel, R., Milliken, G., Stroup, W., and Wolfinger, R. 1996. "SAS Systems for Mixed Models," SAS Institute Inc., Cary, NC.

Liverani, A., Amati, G., and Caligiana, G. 2006. "Interactive Control of Manufacturing Assemblies with Mixed Reality," *Integrated Computer-Aided Engineering* (13:2), pp. 163-172.

Lowry, P. B., Cao, J., and Everard, A. 2011. "Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures," *Journal of Management Information Systems* (27:4), pp. 165-204.

Lowry, P. B., and Moody, G. D. 2015. "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organizational Information Security Policies," *Information Systems Journal* (forthcoming).

Lowry, P. B., Moody, G. D., Galletta, D. F., and Vance, A. 2013. "The Drivers in the Use of Online Whistle-Blowing Reporting Systems," *Journal of Management Information Systems* (30:1), pp. 153-189.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J. L., and Wells, T. 2012. "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers," *Journal of the American Society for Information Science and Technology* (63:4), pp. 755-766.

Lowry, P. B., Nunamaker Jr., J. F., Curtis, A., and Lowry, M. R. 2005. "The Impact of Process Structure on Novice, Internet-Based, Asynchronous-Distributed Collaborative Writing Teams," *IEEE Transactions on Professional Communication* (48:4), pp. 341-364.

Lowry, P. B., Posey, C., Roberts, T. L., and Bennett, R. J. 2014. "Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse," *Journal of Business Ethics* (121:3), pp. 385-401.

Lowry, P. B., Roberts, T. L., Dean, D., and Marakas, G. M. 2009. "Toward Building Self-Sustaining Groups in PCR-Based Tasks through Implicit Coordination: The Case of Heuristic Evaluation," *Journal of the Association for Information Systems* (10:3), pp. 170-195.

Lowry, P. B., Romano, N. C., Jenkins, J. L., and Guthrie, R. W. 2009. "The CMC Interactivity Model: How Interactivity Enhances Communication Quality and Process Satisfaction in Lean-Media Groups," *Journal of Management Information Systems* (26:1), pp. 155-195.

Lowry, P. B., Teh, N., Molyneux, B., and Bui, S. N. 2010. "Using Theories of Formal Control, Mandatoriness, and Reactance to Explain Working Professionals' Intent to Comply with New IT Security Policies," IFIP WG 8.11 / 11.13, The Dewald Roode Workshop on IS Security Research 2010, Waltham, MA, October 8-9, pp. 278-316.

Lowry, P. B., Wilson, D. W., and Haig, W. L. 2014. "A Picture Is Worth a Thousand Words: Source Credibility Theory Applied to Logo and Website Design for Heightened Credibility and Consumer Trust," *International Journal of Human–Computer Interaction* (30:1), pp. 63-93.

Lowry, P. B., Zhang, D., Zhou, L., and Fu, X. 2010. "Effects of Culture, Social Presence, and Group Composition on Trust in Technology-Supported Decision-Making Groups," *Information Systems Journal* (20:3), pp. 297-315.

MacKinnon, D. P. 2008. *Introduction to Statistical Mediation Analysis*, Mahwah, NJ: Lawrence Erlbaum Associates.

MacKinnon, D. P., and Fairchild, A. J. 2009. "Current Directions in Mediation Analysis," *Current Directions in Psychological Science* (18:1), pp. 16-20.

MacKinnon, D. P., Lockwood, C. M., Hoffman, J. M., West, S. G., and Sheets, V. 2002. "A Comparison of Methods to Test Mediation and Other Intervening Variable Effects," *Psychological Methods* (7:1), pp. 83-104.

McLean, R., Sanders, W., and Stroup, W. 1991. "A Unified Approach to Mixed Linear Models," *American Statistician* (45:1991), pp. 54-64.

Mennecke, B. E., Triplett, J. L., Hassall, L. M., Conde, Z. J., and Heer, R. 2011. "An Examination of a Theory of Embodied Social Presence in Virtual Worlds," *Decision Sciences* (42:2), pp. 413-450.

Mondloch, C. J., and Desjarlais, M. 2010. "The Function and Specificity of Sensitivity to Cues to Facial Identity: An Individual-Differences Approach," *Perception* (39), pp. 819-829.

Moore, R. J., Ducheneaut, N., and Nickell, E. 2007. "Doing Virtually Nothing: Awareness and Accountability in Massively Multiplayer Online Worlds," *Computer Supported Cooperative Work* (16:3), pp. 265-305.

Mueller, J., Hutter, K., Fueller, J., and Matzler, K. 2011. "Virtual Worlds as Knowledge Management Platform: A Practice-Perspective," *Information Systems Journal* (21:6), pp. 479-501.

Muller, D., Judd, C. M., and Yzerbyt, V. Y. 2005. "When Moderation Is Mediated and Mediation Is Moderated," *Journal of Personality and Social Psychology* (89:6), pp. 852-863.

O'Fallon, M., and Butterfield, K. 2005. "A Review of the Empirical Ethical Decision-Making Literature: 1996–2003," *Journal of Business Ethics* (59:4), pp. 375-413.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3), pp. 549-584.

Pinsonneault, A., and Barki, H. 1999. "The Illusion of Electronic Brainstorming Productivity: Theoretical and Empirical Issues," *Information Systems Research* (10:4), pp. 378-382.

Piquero, N. L., Exum, M. L., and Simpson, S. 2005. "Integrating the Desire for Control and Rational Choice in a Corporate Crime Context," *Justice Quarterly* (22:2), pp. 252-280.

Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, S. 2010. "Proposing the Online Community Self-Disclosure Model: The Case of Working Professionals in France and the UK Who Use Online Communities," *European Journal of Information Systems* (19:2), pp. 181-195.

Posey, C., Roberts, T. L., Bennett, R., and Lowry, P. B. 2011. "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse," *Journal of Information System Security* (7:1), pp. 24-47.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189-1210.

Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns Between Information Security Profes-

sionals and Ordinary Organizational Insiders," *Information & Management* (51:5), pp. 551-567.

Qiu, L., and Benbasat, I. 2005. "Online Consumer Trust and Live Help Interfaces: The Effects of Text-to-Speech Voice and Three-Dimensional Avatars," *International Journal of Human–Computer Interaction* (19:1), pp. 75-94.

Ramsey, F., and Schafer, D. 2013. *The Statistical Sleuth: A Course in Methods of Data Analysis* (3rd ed.), Boston: Brooks/Cole.

Reicher, S., and Levine, M. 1994. "Deindividuation, Power Relations between Groups and the Expression of Social Identity: The Effects of Visibility to the Out-Group," *British Journal of Social Psychology* (33:1994), pp. 145-163.

Roberts, T. L., Lowry, P. B., and Sweeney, P. D. 2006. "An Evaluation of the Impact of Social Presence through Group Size and the Use of Collaborative Software on Group Member 'Voice' in Face-to-Face and Computer-Mediated Task Groups," *IEEE Transactions on Professional Communication* (49:1), pp. 28-43.

Rodell, J. B., and Judge, T. A. 2009. "Can 'Good' Stressors Spark 'Bad' Behaviors? The Mediating Role of Emotions in Links of Challenge and Hindrance Stressors with Citizenship and Counterproductive Behaviors," *Journal of Applied Psychology* (94:6), pp. 1438-1451.

Rosenberg, M. J. 1968. "When Dissonance Fails: On Eliminating Evaluation Apprehension from Attitude Measurement," *Journal of Personality and Social Psychology* (1:1), pp. 28-42.

Rossi, P. H. 1979. "Vignette Analysis: Uncovering the Normative Structure of Complex Judgments," in *Qualitative and Quantitative Social Research: Papers in Honor of Paul F. Lazarsfeld*, New York: Free Press, pp. 176-186.

Rossi, P. H., and Anderson, A. B. 1982. "The Factorial Survey Approach: An Introduction," in *Measuring Social Judgments: The Factorial Survey Approach,* P. H. Rossi, and S. Nock (eds.), Beverly Hills, CA: Sage Publications, pp. 15-67.

Rossi, P. H., Sampson, W. A., Bose, C. E., Jasso, G., and Passel, J. 1974. "Measuring Household Social Standing," *Social Science Research* (3:3), pp. 169-190.

Schlenker, B., Weigold, M., and Doherty, K. 1991. "Coping with Accountability: Self-Identification and Evaluative Reckonings," in *Handbook of Social and Clinical Psychology: The Health Perspective,* C. R. Snyder, and D. R. Forsyth (eds.), Elmsford, NY: Pergamon Press, pp. 96-115.

Scholten, L., van Knippenberg, D., Nijstad, B., and de Dreu, C. 2007. "Motivated Information Processing and Group Decision-Making: Effects of Process Accountability on Information Processing and Decision Quality," *Journal of Experimental Social Psychology* (43:4), pp. 539-552.

Schopler, J., Insko, C., Drigotas, S., Wieselquist, J., Pemberton, M., and Cox, C. 1995. "The Role of Identifiability in the Reduction of Interindividual-Intergroup Discontinuity," *Journal of Experimental Social Psychology* (31:6), pp. 553-574.

Sedikides, C., Herbst, K. C., Hardin, D. P., and Dardis, G. J. 2002. "Accountability as a Deterrent to Self-Enhancement: The Search for Mechanisms," *Journal of Personality and Social Psychology* (83:3), pp. 592-605.

Seron, C., Pereira, J., and Kovath, J. 2006. "How Citizens Assess Just Punishment for Police Misconduct," *Criminology* (44:4), pp. 925-960.

Shrout, P., and Bolger, N. 2002. "Mediation in Experimental and Nonexperimental Studies: New Procedures and Recommendations," *Psychological Methods* (7:4), pp. 422-445.

Sia, C.-L., Tan, B. C. Y., and Wei, K.-K. 2002. "Group Polarization and Computer-Mediated Communication: Effects of Communication Cues, Social Presence, and Anonymity," *Information Systems Research* (13:1), pp. 70-90.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Siponen, M., and Vance, A. 2014. "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems* (23:3), pp. 289-305.

Sobel, M. E. 1982. "Asymptotic Confidence Intervals for Direct Effects in Structural Equation Models," in *Sociological Methodology*, S. Leinhardt (ed.), Washington, DC: American Sociological Association, pp. 290-312.

Staw, B. M. 1976. "Knee-Deep in the Big Muddy: A Study of Escalating Commitment to a Chosen Course of Action," *Organizational Behavior and Human Processes* (16:1976), pp. 27-44.

Suh, K. S., and Lee, Y. E. 2005. "The Effects of Virtual Reality on Consumer Learning: An Empirical Investigation," *MIS Quarterly* (29:4), pp. 673-697.

Tadmor, C., and Tetlock, P. E. 2009. "Accountability," in *The Cambridge Dictionary of Psychology,* D. Matsumoto (ed.), Cambridge, UK: Cambridge University Press, p. 8.

Tanis, M., and Postmes, T. 2003. "Social Cues and Impression Formation in CMC," *Journal of Communication* (53:4), pp. 676-693.

Tanis, M., and Postmes, T. 2007. "Two Faces of Anonymity: Paradoxical Effects of Cues to Identity in CMC," *Computers in Human Behavior* (23:2), pp. 955-970.

Tetlock, P. E. 1983a. "Accountability and Complexity of Thought," *Journal of Personality and Social Psychology* (45:1), pp. 74-83.

Tetlock, P. E. 1983b. "Accountability and the Perseverance of First Impressions," *Social Psychology Quarterly* (46:4), pp. 285-292.

Tetlock, P. E. 1985. "Accountability: A Social Check on the Fundamental Attribution Error," *Social Psychology Quarterly* (48:3), pp. 227-236.

Tetlock, P. E. 1992. "The Impact of Accountability on Judgment and Choice: Toward a Social Contingency Model," *Advances in Experimental Social Psychology* (25:1992), pp. 331-376.

Tetlock, P. E. 1999. "Accountability Theory: Mixing Properties of Human Agents with Properties of Social Systems," in *Shared Cognition in Organizations: The Management of Knowledge,* L. L. Thompson, J. M. Levine, and D. M. Messick (eds.), Hillsdale, NJ: Lawrence Erlbaum Associates, pp. 117-138.

Tetlock, P. E., and Boettger, R. 1989. "Accountability: A Social Magnifier of the Dilution Effect," *Journal of Personality and Social Psychology* (57:3), pp. 388-398.

Tetlock, P. E., and Boettger, R. 1994. "Accountability Amplifies the Status-Quo Effect When Change Creates Victims," *Journal of Behavioral Decision Making* (7:1), pp. 1-23.

Tetlock, P. E., and Kim, J. I. 1987. "Accountability and Judgment Processes in a Personality Prediction Task," *Journal of Personality and Social Psychology* (52:4), pp. 700-709.

Tetlock, P. E., Skitka, L., and Boettger, R. 1989. "Social and Cognitive Strategies for Coping with Accountability: Conformity, Complexity, and Bolstering," *Journal of Personality and Social Psychology* (57:4), pp. 632-640.

Trevino, L. K. 1992. "Experimental Approaches to Studying Ethical–Unethical Behavior in Organizations," *Business Ethics Quarterly* (2:2), pp. 121-136.

Vance, A., Elie-Dit-Cosaque, C., and Straub, D. W. 2008. "Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture," *Journal of Management Information Systems* (24:4), pp. 73-100.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-289.

Wallander, L. 2009. "25 Years of Factorial Surveys in Sociology: A Review," *Social Science Research* (38:3), pp. 505-520.

Walther, J. B. 1992. "Interpersonal Effects in Computer-Mediated Interaction: A Relational Perspective," *Communication Research* (19:1), pp. 52-90.

Walther, J. B., Slovacek, C. L., and Tidwell, L. C. 2001. "Is a Picture Worth a Thousand Words? Photographic Images in Long-Term and Short-Term Computer-Mediated Communication," *Communication Research* (28:1), pp. 105-134.

Ward, P., and Smith, C. L. 2002. "The Development of Access Control Policies for Information Technology Systems," *Computers and Security* (21:4), pp. 356-371.

Whetten, D. A. 1989. "What Constitutes a Theoretical Contribution?," *Academy of Management Review* (14:4), pp. 490-495.

Whetten, D. A. 2009. "Modeling Theoretical Propositions," in *Designing Research for Publication,* A. S. Huff (ed.), Thousand Oaks, CA: Sage Publications, Inc., pp. 490-495.

Williams, K., Harkins, S., and Latane, B. 1981. "Identifiability as a Deterrent to Social Loafing: Two Cheering Experiments," *Journal of Personality and Social Psychology* (40:1981), pp. 303-311.

Wirth, W., Bocking, T., Karnowski, V., and von Pape, T. 2007. "Heuristic and Systematic Use of Search Engines," *Journal of Computer–Mediated Communication* (12:3), pp. 778-800.

Zajonc, R. 1980. "Feeling and Thinking: Preferences Need No Inferences," *American Psychologist* (35:1980), pp. 151-175.

Zhang, P., and Galletta, D. 2006. *Human–Computer Interaction and Management Information Systems: Foundations*, Armonk, NY: M. E. Sharpe, Inc.

About the Authors

Anthony Vance is as an assistant professor of Information Systems in the Marriott School of Management of Brigham Young University. He has earned Ph.D. degrees in Information Systems from Georgia State University, USA; University of Paris—Dauphine, France; and University of Oulu, Finland. He received a B.S. in IS and Master's of Information Systems Management (MISM) from Brigham Young University, during which he was also enrolled in the IS Ph.D. preparation program. His previous experience includes working as a visiting research professor in the Information Systems Security Research Center at the University of Oulu. He also worked as an information security consultant and fraud analyst for Deloitte. His work is published in outlets such as *MIS Quarterly*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, and *Journal of the American Society for Information Science and Technology*, as well as in the proceedings of the ACM Conference on Human Factors in Computing Systems. His research focuses on behavioral and neuroscience applications to information security.

Paul Benjamin Lowry is a Full Professor of Information Systems at the Department of Information Systems, City University of Hong Kong where he is also the Associate Director of the MBA program. He received his Ph.D. in Management Information Systems from the University of Arizona. He has published articles in journals including *MIS Quarterly*, *Information Systems Research*, *Journal of MIS*, *Journal of the AIS, Information Systems Journal*, *European Journal of Information Systems*, *International Journal of Human–Computer Studies*, *Information & Management*, *Communications of the ACM*, *Information Sciences*, *Decision Support Systems,* and *Communications of the AIS*. He serves as an associate editor for *European Journal of Information Systems*, *Information & Management*, *Communications of the AIS*, and *Information Security Education Journal*, and as a senior editor for *AIS Transactions on HCI*. He has also served as a track chair for ICIS, ECIS, and PACIS. His research interests include behavioral security issues, HCI, e-commerce, and scientometrics.

Dennis Eggett is an associate research professor of statistics at Brigham Young University. He earned a Ph.D. in statistics at North Carolina State University and an M.S. and B.S. in applied statistics at Brigham Young University. He previously worked for U.S. government contractor Pacific Northwest National Laboratory and for SAS Institute. His research interests include linear statistical models, multivariate statistics, mixed models, and logistic regression. He has published over 100 refereed articles in journals such as *Advances in Accounting Behavioral Research*, *Journal of Transportation Engineering*, *Journal of Clinical Psychology*, *Journal of Leisure Research*, *Environmental and Experimental Botany*, and *Analytical Biochemistry*.

MIS Quarterly

RESEARCH ARTICLE

INCREASING ACCOUNTABILITY THROUGH USER-INTERFACE DESIGN ARTIFACTS: A NEW APPROACH TO ADDRESSING THE PROBLEM OF ACCESS-POLICY VIOLATIONS

Anthony Vance
Information Systems Department, Marriott School of Management, Brigham Young University,
Provo, UT 84602 U.S.A. {anthony@vance.name}

Paul Benjamin Lowry
College of Business, City University of Hong Kong, 83 Tat Chee Avenue,
Kowloon Tong, Hong Kong CHINA {Paul.Lowry.PhD@gmail.com}

Dennis Eggett
Department of Statistics, Brigham Young University, Provo, UT 84602 U.S.A. {theegg@stat.byu.edu}

Appendix A

Comparing Accountability and Deterrence

In this appendix we compare and contrast accountability theory and deterrence theory, which have some conceptual and operational overlap and exhibit important differences. These similarities and dissimilarities are summarized in Table A1.

Table A1. Accountability Theory and Deterrence Theory Compared

Element	Deterrence Theory	Accountability Theory
Objective of theory	Explains how to reduce antisocial behaviors.	Explains how to reduce antisocial behaviors or increase prosocial behaviors.
Central mechanism	Sanctions.	Self-image preservation and social desirability.
External component	Externally imposed sanctions.	Person or organization to whom one must account.
Internal component	Cost-benefit analysis. Self-imposed sanction (shame).	Self-image preservation.
Partially operationalizable via monitoring?	Yes—used to increase certainty of sanctions.	Yes—used to evaluate employee performance.
Certainty	Greater certainty of sanctions is better than less certainty, but does not explain how certainty can be increased.	Explains submanipulations of accountability: • Identifiability (having one's actions linked to oneself). • Evaluation (having one's actions assessed by another person). • Justification (having to give reasons for one's behavior).

Deterrence theory is the most widely applied theoretical perspective in behavioral IS security, having been applied in more than 17 studies (see D'Arcy and Herath 2011). Deterrence theory, a classical theory of criminology first described by Cesare Beccaria (1738-1794) and Jeremy Bentham (1748-1832), predicts that an increase in the perception of severity, celerity, and certainty of sanctions for a potential offense increases the perceived costs of an act, thus decreasing its desirability (Gibbs 1975; Tittle 1980). In addition to externally imposed formal sanctions, modern conceptions of deterrence theory have included informal sanctions, such as disapproval from peers (D'Arcy and Devaraj 2012; Paternoster and Simpson 1996) and shame, which is considered a self-imposed sanction (Pratt et al. 2006; Siponen and Vance 2010).

Accountability Theory and Deterrence Theory Contrasted

Accountability is distinct from deterrence in several ways. First, accountability and deterrence theory differ in their objectives. Whereas both accountability and deterrence theory explain how to reduce antisocial behaviors (D'Arcy and Hovav 2009; Sedikides et al. 2002), accountability theory also explains how to increase prosocial behaviors (Fandt and Ferris 1990). The prosocial behaviors may include higher conformity to expected behaviors (Tetlock et al. 1989), enhanced employee empowerment (Wallace et al. Mathe 2011), facilitated trust (Ammeter et al. 2004; Tetlock 1985), and increased work performance (Wallace et al. 2011). That accountability can also be used to promote positive behaviors suggests that a mechanism distinct from deterrence is at work.

Second, accountability and deterrence theory differ in their central mechanisms. Deterrence involves a cost–benefit analysis of the benefit of committing a norm-breaking act weighed against the severity and certainty of a sanction (Becker 1974; D'Arcy and Herath 2011). Whereas accountability may also involve an element of certainty (i.e., the likelihood of having to give an account), its central mechanisms are self-image preservation and social approval (Gelfand and Realo 1999; Tetlock 1999). These mechanisms can be effective even when no defined relationship exists between the respondent and the other person to whom one may be expected to justify oneself (Guerin 1989). The expectation of having to give an account and be evaluated by another person has been shown to be sufficient to deter undesirable behaviors, even when sanctions are not involved (Sedikides et al. 2002). Thus, whereas sanctions are at the heart of deterrence theory, accountability is still effective even when sanctions are not involved.

Third, both accountability and deterrence have internal and external components, although these components are different. For deterrence theory, the external component is a sanction that is externally imposed. In addition to an internal cost–benefit analysis, modern deterrence theory includes shame as a self-imposed sanction that may be purely internal—that is, not initiated by an outside party (D'Arcy and Herath 2011). In contrast, for accountability theory, the external component is the person to whom one expects to give an account, whereas self-image preservation is an internal exercise (at least initially, before action is prompted) (Gelfand and Realo 1999).

Both deterrence and accountability are at least partially operationalizable via the use of sanctions. However, whereas deterrence suggests the use of monitoring to increase the certainty of sanctions (D'Arcy et al. 2009; Parker 1998), accountability advises monitoring as the basis for a possible future evaluation (Gelfand et al. 2004). Therefore, although the monitoring mechanism may be similar in both cases, the central mechanism that is facilitated is different (i.e., sanctions versus evaluation). For example, monitoring can be used as an accountability mechanism to encourage and award employee performance (Hall et al. 2003).

For the purposes of the present study, however, the most relevant difference between deterrence and accountability is that deterrence theory suggests that greater certainty is better than less certainty, even though the theory itself doesn't explain how certainty should be increased (Gibbs 1975). In contrast, accountability theory explains several theoretical submanipulations—including the presence of another, identifiability, evaluation, and reason giving—each of which can be directly manipulated (Lerner and Tetlock 1999). Because the goal of this research study was to develop UI artifacts that could influence access-policy violation behavior, accountability was chosen as a theoretical guide for the development of the UI artifacts.

Appendix B

Scenarios and Instruments

Table B1. Instructional Scenarios

# / Policy	Scenario Text
1–Against policy	Tom works in the university records office. A woman approaches his desk and asks for her husband's academic transcript. She explains that she is submitting her husband's graduate school applications today and that her husband is traveling, doing campus interviews. She needs to send the transcript today so it can be received before the deadline passes. Although Tom believes doing so may be a violation of university policy, he gives the woman a copy of her husband's transcript.
2–Against policy	Karen works in the advisement center of her college. She is approached by a friend who has a daughter attending the university. The friend is concerned about his daughter's performance in her classes. He says that she has been struggling with depression but won't talk about her problems. He is worried that she is not receiving the help she needs and may be failing her courses. He asks Karen to look up his daughter's grades for the last few semesters to see if things are okay. Although Karen believes doing so may be a violation of university policy, she accesses the daughter's records and relates how she is doing in her coursework.
3–Against policy	Janice is the administrative assistant for her college. She is approached by a professor in her college who is asking for her help. The professor is conducting a research study involving students in the college. The professor has collected the data, and now needs basic demographic information. He asks Janice for the age, GPA, and year in school for the students who participated in the study. Although Janice believes doing so may be a violation of university policy, she gives the professor the demographic information for the students who participated in the study.
4–Against policy	Ethan is a university employee with access to the university records system. He knows Jason, a sophomore who now attends the university. In high school, Jason was very successful academically. Ethan is curious to know how well Jason is doing now that he is at the university. Ethan routinely looks up student information for his work, so accessing Jason's record would not be unusual. Although Ethan believes doing so may be a violation of university policy, he accesses Jason's student record.
5–No policy stated	Tom works in the university records office. A woman approaches his desk and asks for her husband's academic transcript. She explains that she is submitting her husband's graduate school applications today and that her husband is traveling, doing campus interviews. She needs to send the transcript today so it can be received before the deadline passes. Tom gives the woman a copy of her husband's transcript.

Table B1. Instructional Scenarios

# / Policy	Scenario Text
6–No policy stated	Karen works in the advisement center of her college. She is approached by a friend who has a daughter attending the university. The friend is concerned about his daughter's performance in her classes. He says that she has been struggling with depression but won't talk about her problems. He is worried that she is not receiving the help she needs and may be failing her courses. He asks Karen to look up his daughter's grades for the last few semesters to see if things are okay. Karen accesses the daughter's record and relates how she is doing in her coursework.
7–No policy stated	Janice is the administrative assistant for her college. She is approached by a professor in her college who is asking for her help. The professor is conducting a research study involving students in the college. The professor has collected the data, and now needs basic demographic information. He asks Janice for the age, GPA, and year in school for the students who participated in the study. Janice gives the professor the demographic information for the students who participated in the study.
8–No policy stated	Ethan is a university employee with access to the university records system. He knows Jason, a sophomore who now attends the university. In high school, Jason was very successful academically. Ethan is curious to know how well Jason is doing now that he is at the university. Ethan routinely looks up student information for his work, so accessing Jason's record would not be unusual. Ethan accesses Jason's student record.

Table B2. Instrument Documentation

Construct	Item	Source of Item
Intention	1. What is the chance that you would do what the employee did in the described scenario? 0% chance to 100% chance, 11-point scale	Siponen and Vance (2010)
	2. I would act in the same way as the employee did if I was in the same situation. 0% chance to 100% chance, 11-point scale	Vance et al. (2012)
Accountability (pre-vignette)	1. I am held accountable for my actions in the ARS system.	Hochwarter et al. (2005)
	2. University administration/management holds me accountable for all of my actions in the ARS system.	Hochwarter et al. (2005)
	3. I believe that I am accountable for my actions in the ARS system.	New item
Accountability (post-vignette)	1. I would be held accountable for my actions in the ARS system.	Hochwarter et al. (2005)
	2. University administration/management would hold me accountable for all of my actions in the ARS system.	Hochwarter et al. (2005)
	3. I believe that I would be accountable for my actions in the ARS system.	New item
Moral intensity	1. The overall harm (if any) done as a result of what [the scenario character] did would be very small.	Singhapakdi et al. (1996)
	2. There is a very small likelihood that what [the scenario character] did will actually cause any harm.	Singhapakdi et al. (1996)
	3. What [the scenario character] did will not cause any harm in the immediate future.	Singhapakdi et al. (1996)
	4. What [the scenario character] did will harm very few people (if any).*	Singhapakdi et al. (1996)
Subjective norms	1 (reversed). If I did what [the scenario character] did, most of the people who are important to me would respond as follows: Strongly disapprove to strongly approve, 7-point scale	Peace et al. (2003)
	2. Most people who are important to me would look down on me if I did what the employee in the scenario did. Very unlikely to very likely, 7-point scale	Peace et al. (2003)
	3. No one who is important to me thinks it would be okay to do what the employee in the scenario did. Strongly disagree to strongly agree, 7-point scale	Peace et al. (2003)
Impulsivity	1. I act on impulse.	Pogarsky (2004)
	2. I often do things on the spur of the moment.	Pogarsky (2004)
	3 (reversed). I always consider the consequences before I take action.	Pogarsky (2004)
	4 (reversed). I rarely make hasty decisions.	Pogarsky (2004)
Organizational trust	1. I believe my organization has high integrity.	Robinson (1996)
	2. I can expect my organization to treat me in a consistent and predictable fashion.	Robinson (1996)
	3. My organization is open and up-front with me.	Robinson (1996)

Note: Unless stated otherwise, items were measured on a 7-point scale from “strongly disagree” to “strongly agree.”
*Dropped to improve factorial validity.

Appendix C

Our Research in Context of Design Science

Here, we further describe the design science contributions of our study in view of the latest literature. Although there is no single authoritative or required approach to design science, common among seminal frameworks of design science is the notion that some of the major contributions an IS design science paper can make include describing and defining both the problem space and a conceptual solution, which can be described in terms of proof-of-concept and proof-of-value (Gregor and Hevner 2013; Hevner et al. 2004; Nunamaker and Briggs 2011; Nunamaker et al. 2013; Twyman et al. 2015). Hence, to better understand our design science contribution in the context of the literature, it is first important to understand proof-of-concept and proof-of-value. *Proof-of-concept* is the point at which enough evidence exists to show that the described conceptual solution of design is feasible and promising, at least in a limited context (Nunamaker and Briggs 2011; Nunamaker et al. 2013). In contrast, *proof-of-value* is achieved when researchers show that an IT artifact actually works in reality (Nunamaker and Briggs 2011; Nunamaker et al. 2013). These are most recently demonstrated and described in Twyman et al. (2015).

Importantly, proof-of-concept should be established from an IT artifact and design-science perspective before proof-of-value is established, and both are necessary in science (Gregor and Hevner 2013; Hevner et al. 2004; Nunamaker and Briggs 2011; Nunamaker et al. 2013). Both contributions are important but are not the same in terms of advancing design science and theory (Gregor and Hevner 2013; Hevner et al. 2004; Nunamaker and Briggs 2011; Nunamaker et al. 2013).

We now explain these details in the context of our research and specify the key differences between and contributions of the present study and that of Vance et al. (2013). Hence, from a design science and a theoretical contribution perspective, we submit that the work in Vance et al. helps establish proof-of-concept whereas the present study helps establish proof of value.

Specifically, Vance et al. advance the idea that in a scenario-based study, highlighting four subdimensions of accountability, will cause respondents to develop a negative correlation with intention to commit access-policy violations. Despite their novelty, the findings of Vance et al. are limited in three important ways. First, they test the concept of accountability using hypothetical, text-based scenarios in which each participant imagined for her/himself what the accountability UI mechanisms might look like and how such mechanisms might make them feel. Therefore, the study by Vance et al. does not demonstrate how to actually incorporate accountability into UI designs, and their results do not necessarily accurately reflect how users respond to actual UI mechanisms of accountability.

Second, although Vance et al. find a negative association between the four accountability mechanisms and intentions to violate the access policy, they do not measure perceptions of accountability directly. Rather, the effect of the mechanisms on accountability is only implied. Therefore, it is not clear whether the mechanisms can actually increase perceptions of accountability as theorized. Without such evidence, the role and influence of accountability in their model continues to be unresolved.

Third, and building off of the point above, Vance et al. imply that accountability itself can reduce access-policy violations. However, they neither theoretically support nor empirically test this assertion. It is therefore unknown whether the construct of accountability itself influences intentions to violate the access policy. This is an all-too-frequent gap in the accountability literature—implicating the role of accountability but not measuring it directly (Lerner and Tetlock 1999). This also illustrates the importance of the "science" element in design science, in building toward proof-of-value.

Fourth, although Vance et al. speculate that accountability mediates the effects of the UI mechanism on intention, these relationships were also untested. This is a critical limitation, because if accountability is not tested as a mediator, we cannot be certain whether the UI mechanisms actually influence behavior through the lever of accountability or whether their impact is through some other construct, such as deterrence, fear, or uncertainty. If accountability theory holds in a novel UI context, then accountability itself should act in a key mediation role between manipulated UI artifacts designed to increase identifiability, monitoring, evaluation, and social presence. That is, accountability should act as the underlying causal-process mechanism that ties UI artifacts to changes in intentions and subsequent behavior. However, not only is this not addressed in Vance et al., but nowhere in the accountability literature has accountability itself been established empirically as a causal mediator.

The present study addresses these four gaps and moves from proof-of-concept to proof-of-value in the following ways. First, we develop UI design artifacts that reify the four subdimensions of accountability within the user interface of a broad-access system. In this way, we can evaluate how users respond to the graphical UI manipulations to which they are exposed. Second, we measure perception of accountability to directly examine its effects on intention to violate the access policy. Third, we examine whether perceived accountability mediates the effects

of the UI design artifacts on intention to violate the access policy. Fourth, we use actual employees who employ the target system in their day-to-day work and who are prone to accountability violations because the system is an open-access system. Table C1 summarizes and describes the differences between the articles with respect to proof-of-concept and proof-of-value.

Table C1. Illustrating Proof-of-Concept and Proof-of-Value in the Research Stream

Key Design Element	Vance et al. (2013): Example of Proof-of-Concept	This Article: Example of Proof-of-Value	Additive Insights Gained from Proof-of-Value
UI design artifacts (RQ1)	Used accountability theory to identify four mechanisms to decrease access-policy violations. Did not instantiate the mechanisms.	Instantiated mechanisms as four UI design artifacts. Evaluated these artifacts within the context of system in use.	Offers a proof-of-value for the implementation of UI design artifacts.
Influence of UI design artifacts on accountability (RQ1)	Theorized that accountability mechanisms would increase perceptions of accountability. Did not test this relationship (perceptions of accountability were not measured).	Measured perceptions of accountability directly. Measured the impact of UI design artifacts on perceived accountability.	UI design artifacts effectively increase perceptions of accountability.
Influence of accountability on access policy–violation intentions (RQ2)	Theorized that perceived accountability can reduce intentions to violate the access policy. Did not test this relationship.	Showed that increases to perceived accountability reduce intentions to violate the access policy.	Perceived accountability is an effective mechanism to reduce ISP policy violations, and a viable alternative to deterrence approaches.
Mediation effect of perceived accountability (RQ3)	Tested the direct effects of accountability mechanisms on intention. Implied that perceived account-ability mediates the effects of accountability mechanisms on intention to violate. Did not theorize or test this relationship.	Theorized and empirically demonstrated that perceived accountability does mediate the effects of the UI design artifacts.	The UI design artifacts impact intention to violate through the operation of perceived accountability, rather than having individual effects on intention. Solidifies the theoretical and practical importance of accountability to reduce ISP violations.
Context	Less realistic and preliminary: (1) used textual, non-graphical scenarios; (2) used students; (3) system had no real-life relationship with participants	(1) used graphical screen manipulations from real system; (2) used employees who worked daily on the same open-access system.	These ideas work with the target audience in the field, not just in the lab.

References

Ammeter, A. P., Douglas, C., Ferris, G. R., and Goka, H. 2004. "A Social Relationship Conceptualization of Trust and Accountability in Organizations," *Human Resource Management Review* (14:1), pp. 47-65.

Becker, G. 1974. "Crime and Punishment: An Economic Approach," in *Essays in the Economics of Crime and Punishment,* G. S. Becker, and W. M. Landes (eds.), Washington, DC: The National Bureau of Economic Research, pp. 169-217.

D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), pp. 1091-1124.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643–658.

D'Arcy, J., and Hovav, A. 2009. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics* (89:1), pp. 59-71.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Fandt, P., and Ferris, G. 1990. "The Management of Information and Impressions: When Employees Behave Opportunistically," *Organizational Behavior and Human Decision Processes* (45:1990), pp. 140-158.

Gelfand, M., and Realo, A. 1999. "Individualism-Collectivism and Accountability in Intergroup Negotiations," *Journal of Applied Psychology* (84:5), pp. 721-736.

Gelfand, M. J., Lim, B.-C., and Raver, J. L. 2004. "Culture and Accountability in Organizations: Variations in Forms of Social Control across Cultures," *Human Resource Management Review* (14:1), pp. 135-160.

Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence*, New York, NY: Elsevier.

Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly* (37:2), pp. 337-355.

Guerin, B. 1989. "Reducing Evaluation Effects in Mere Presence," *Journal of Social Psychology* (129:2), pp. 182-190.

Hall, A., Frink, D., Ferris, D., Hochwarter, G., Kacmar, C., and Bowen, M. 2003. "Accountability in Human Resources Management," in *New Directions in Human Resource Management,* L. L. Neider, and C. A. Schriesheim (eds.), Greenwich, CT: Information Age Publishing, pp. 29-63.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75-105.

Hochwarter, W. A., Perrewé, P. L., Hall, A. T., and Ferris, G. R. 2005. "Negative Affectivity as a Moderator of the Form and Magnitude of the Relationship between Felt Accountability and Job Tension," *Journal of Organizational Behavior* (26:5), pp. 517-534.

Lerner, J. S., and Tetlock, P. E. 1999. "Accounting for the Effects of Accountability," *Psychological Bulletin* (125:2), pp. 255-275.

Nunamaker Jr., J. F., and Briggs, R. O. 2011. "Toward a Broader Vision for Information Systems," *ACM Transactions on Management Information Systems* (2:4), pp. 1-12.

Nunamaker Jr., J. F., Twyman, N. W., and Giboney, J. S. 2013. "Breaking out of the Design Science Box: High-Value Impact through Multidisciplinary Design Science Programs of Research," in *Proceedings of the 19th Americas Conference on Information Systems*, Chicago, IL.

Parker, D. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*, Hoboken, NJ: Wiley Computer Publishing.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3), pp. 549-584.

Peace, A. G., Galletta, D. F., and Thong, J. Y. L. 2003. "Software Piracy in the Workplace: A Model and Empirical Test," *Journal of Management Information Systems* (20:1), pp. 153-177.

Pogarsky, G. 2004. "Projected Offending and Implications for Heterotypic Continuity," *Criminology* (42:1), pp. 111-135.

Pratt, T., Cullen, F., Blevins, K., Daigle, L., and Madensen, T. 2006. "The Empirical Status of Deterrence Theory: A Meta-Analysis," in *Taking Stock: The Status of Criminological Theory: Advances in Criminological Theory,* F. Cullen, J. p. Wright, and K. Blevins (eds.), New Brunswick, NJ: Transaction Books, pp. 367-395.

Robinson, S. L. 1996. "Trust and Breach of the Psychological Contract," *Administrative Science Quarterly* (41:4), pp. 574-599.

Sedikides, C., Herbst, K. C., Hardin, D. P., and Dardis, G. J. 2002. "Accountability as a Deterrent to Self-Enhancement: The Search for Mechanisms," *Journal of Personality and Social Psychology* (83:3), pp. 592-605.

Singhapakdi, A., Vitell, S., and Kraft, K. 1996. "Moral Intensity and Ethical Decision-Making of Marketing Professionals," *Journal of Business Research* (36:3), pp. 245-255.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Tetlock, P. E. 1985. "Accountability: A Social Check on the Fundamental Attribution Error," *Social Psychology Quarterly* (48:3), pp. 227-236.

Tetlock, P. E. 1999. "Accountability Theory: Mixing Properties of Human Agents with Properties of Social Systems," in *Shared Cognition in Organizations: The Management of Knowledge,* L. L. Thompson, J. M. Levine, and D. M. Messick (eds.), Hillsdale, NJ: Lawrence Erlbaum Associates, pp. 117-138.

Tetlock, P. E., Skitka, L., and Boettger, R. 1989. "Social and Cognitive Strategies for Coping with Accountability: Conformity, Complexity, and Bolstering," *Journal of Personality and Social Psychology* (57:4), pp. 632-640.

Tittle, C. R. 1980. *Sanctions and Social Deviance: The Question of Deterrence*, Westport, CT: Praeger.

Twyman, N. W., Lowry, P. B., Burgoon, J. K., and Nunamaker Jr., J. F. 2015. "Autonomous Scientifically Controlled Screening Systems for Detecting Information Purposely Concealed by Individuals," *Journal of Management Information Systems* (31:3), forthcoming.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-289.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information and Management* (49:3-4), pp. 190-198.

Wallace, J. C., Johnson, P. D., and Mathe, K. 2011. "Structural and Psychological Empowerment Climates, Performance, and the Moderating Role of Shared Felt Accountability: A Managerial Perspective," *Journal of Applied Psychology* (96:4), pp. 840-850.