Reducing Unauthorized Access by Insiders through User Interface Design: Making End Users Accountable

Anthony Vance  
Brigham Young University  
anthony@vance.name

Braden Molyneux  
University of British Columbia  
bradenex@gmail.com

Paul Benjamin Lowry  
City University of Hong Kong  
paul.lowry.phd@gmail.com

Abstract

A long-time tenet of information security is the principle of least privilege, which requires that systems users be given the minimum amount of access privilege required to complete a task. However, many financial, medical, and customer records systems grant employees broad access for reasons of practical necessity. Unfortunately, with broad access rights comes potential for abuse.

This paper investigates how user interface design features of a system can be designed to make end users feel more accountable for their actions in the system and less likely to abuse their access rights. To do so, we developed a factorial survey to determine the effects of user interface design features relating to three aspects of accountability: (1) identifiability, (2) evaluation, and (3) social presence. The results of the factorial survey show that the accountability design features significantly reduced intention to commit unauthorized access.

1. Introduction

A long-standing tenet of information security is the principle of least privilege, the concept that “every privileged user of the system should operate using the least amount of privilege necessary to complete the job” [42, p. 389]. However, many medical, financial, and personnel records systems are intentionally deployed with seemingly little regard for this principle. Rather than limiting access to specific areas, end users of these systems are given broad access to information.

Unsurprisingly, with this broad access comes potential for abuse. For example, the Integrated Data Retrieval System (IDRS) used by U.S. Internal Revenue Service (IRS) allows auditors to view tax records of individuals they are not assigned to audit [25]. Although flexible, this broad access posses a “persistent vulnerability for the IRS” [58, p. 36]. In a one year period between April 2009 and March 2010, 439 IRS employees were terminated or formally sanctioned for unauthorized access violations in the system made out of curiosity or for personal gain [58, 57]. Abuses by users of medical and customer records systems are similarly frequent [41, 10].

If the potential for abuse of private information is so great, why is the principle of least privilege not more strictly employed in these systems? One reason is practical necessity. According to one hospital administrator, the problem is stated as follows: “There are just thousands of people who have access—and need to have access—to confidential information, and to try to change their behavior is a challenge” [41, p. D1].

One promising means for modifying the behaviors of end users with broad access privileges is through accountability, which is “the implicit or explicit pressure to justify one’s beliefs and actions to others” [54, p. 8]. The construct of accountability has received substantial attention in fields of psychology and organizational behavior [28, 48]. Prior research has consistently found that a person’s expectation that he/she will be held accountable reduces the likelihood the person will behave in socially unacceptable ways [18].

Although the potential of IT systems to foster accountability has long been recognized [65], to date no research has examined the effects of accountability within the field of Information Systems. The research question of the proposed study is therefore the following:

RQ: How can features of an information system be designed to increase perceptions of accountability and thereby deter IS policy violations?

2. Theory

2.1 Access Policy Violations—the Dependent Variable

The dependent variable of interest in this study is access policy violations by end users. Research on IS security policy violations was presage by research on computer abuse, which is defined as “the unauthorized
and deliberate misuse of assets of the local organizational information system by individuals”, including misuse of hardware, software, data, and computer services [53, p. 257, 11]. IS security policy violations are a specific form of computer abuse in that IS security policies explicitly stipulate appropriate and inappropriate usage of systems. Violations of IS security policies are therefore not only deliberate, but consciously contrary to the expressly stated norm of the organization [51].

In this study, the specific type of IS security policy violation chosen are access policy violations—the accessing of information contrary to explicitly stated policies for how access rights may be used. For example, an organization may stipulate that personnel records within a system may only be accessed when they are legitimately required to complete a task [41]. Here it is not a question of whether someone has access rights to something, but whether the use of access rights is according to organizational policy.

2.2. Accountability as a Deterrent

A promising means to deter access policy violations is accountability theory [55], which explains how the perceived need to justify one’s behaviors causes one to consider—and to feel accountable for—the process by which decisions and judgments were reached [29]. This in turn increases the likelihood that one will think deeply and systematically about their procedural behaviors—as opposed to automatic or heuristic behaviors—creating a greater emphasis on creating effective outcomes for which the person is accountable [46].

This increased accountability to process and outcome, along with related systematic processing, is more likely to increase prosocial behaviors [13], increase conformity to expected behaviors [56], increase expected job performance [45], increase conservatism [52], and decrease risk-taking [45].

Our theoretical context focuses on what system-related mechanisms can increase perceptions of accountability in individuals who are working within systems in which they are granted broad access rights. Given the above explanation of the causal mechanisms of accountability, we posit that those who perceive themselves to be accountable for use of their access rights will be more likely to experience the systematic processing and awareness that will increase conservative and prosocial behaviors. That is, they will be less likely to engage in policy violations than those who perceive themselves to be less accountable and thus lean toward heuristic processing of their behaviors.

2.3. Conceptualizing Accountability

Accountability is not a unitary phenomenon, but rather is composed of several subconstructs. Lerner and Tetlock note that “even the simplest accountability manipulation necessarily implicates several empirically distinguishable submanipulations”, including the presence of another, identifiability, evaluation, and reason-giving [29, p. 255].

Of these, identifiability, evaluation, and social presence are particularly amenable to manipulation by system-related mechanisms because of the potential of IT to monitor and/or record behavior [65, 19]. For this reason, this study focuses on how manipulations of identifiability, evaluation, and social presence can be used to deter access policy violations.

2.4. Identifiability

Identifiability is a person’s “knowledge that his outputs could be linked to him” [61, p. 309]. Identifiability is the opposite of anonymity [47], and has been shown to be a potent deterrent of anti-social behaviors [36], as people modify their behavior if they believe that their identify may be recognized [37]. Identifiability is closely related to the construct of deindividuation, which is a person's belief that his/her actions within a group cannot be associated with him/her individually. Numerous studies have found that when people feel deindividuated, “a lowered threshold of normally restrained behavior” results [64]. Conversely, when individuals sense that they are individuated—that is, distinguishable within a group—anti-social behaviors are curtailed [12, 14, 37].

We posit that identifiability will increase perceptions of accountability whereas lack of identifiability will decrease perceptions of accountability. These predictions are explained as follows: Identifiability is an important facilitator of accountability because a person knows his/her actions are able to be linked to him/her, and can therefore be made responsible for those actions [29]. Accordingly, when one is performing behaviors that are identifiable, one is more likely to engage in systematic processing to ensure that only behavior is performed for which the person is willing to be responsible.

Given this theoretical background, we predict in our context that the more identifiability features that are built into a system in which access rights are held, the greater the perception of accountability by users of the system. Subsequently, this increased sense of internal accountability will lead to less access policy violations. In contrast, the less identifiability that is built into a system, the less the perception of accountability will be. Subsequently, a lower
perception of accountability is more likely to be associated with increased computer abuse. Thus we hypothesize:

H1. Identifiability will reduce intention to violate the access policy.

2.5. Evaluation

Evaluation is the expectation that one’s “performance will be assessed by another according to some normative ground rules and with some implied consequences” [29, p. 255]. Naturally, in order for one to come to an expectation of evaluation, one must be aware that one’s performance or actions might be observed either directly or indirectly. Therefore, our research in this area focuses on these two fundamental constructs: (1) logging or observation of behavior, and (2) the expectation of being evaluated based on the behavior observed or recorded.

Studies have shown that expectation of evaluation increases socially desirable behaviors [29, 24] and deters socially undesirable ones [49]. The expectation of evaluation creates evaluation apprehension [16], a state of mind in which self-focused attention is increased. In this state, self-focus heightens awareness of discrepancies of behaviors from espoused standards [49]. In addition, the need to maintain a good impression of oneself in the minds of others demands that negative evaluations be avoided that would undermine self-presentation efforts [3].

The ability to evaluate someone’s behaviors is wholly dependent on one’s awareness of those behaviors. We therefore posit that systems—in particular—can be very effective in enhancing perceptions of evaluation, and therefore also of accountability due to the capability of systems to track behavior at a granular level [17]. Thus, a crucial element to evaluation, and one common in the IT realm, is logging of an individual’s actions within a system, including recording websites visited, records changed, emails sent and received, and a variety of other behaviors. Importantly, however, unless someone is made aware of that he/she is being logged, evaluation apprehension will not occur and the effects of evaluation on accountability will not be evident. Thus the expectation of evaluation must be salient if negative behaviors are to be deterred. From the foregoing, we state the expected hypothesized effects as follows:

H2: Awareness of logging will reduce intention to violate the access policy.
H3: Expectation of evaluation will reduce intention to violate the access policy.

2.6. Electronic Presence

Lerner and Tetlock [29] include the “mere presence of another” as an empirically distinguishable submanipulation of accountability. Research regarding the effects of the presence of another individual is extensive. In fact, Guerin [23] reviewed over 280 studies regarding “mere presence” and its social facilitation effects. Social facilitation “concerns the effects on behavior caused by the presence of other persons” [23, p. 38]. One basic concept of social facilitation is that in the presence of another, an individual has a higher probability of resorting to his or her dominant response [63]. This results in increased performance when executing simple tasks, but reduced performance when performing complex or unfamiliar tasks [22]. However, effects of social facilitation are numerous depending on situational dynamics and other factors as Guerin showed in his review [23]. More recent studies have demonstrated these effects and offered theories as to their causes. Several of these theories lend strong support to our following hypothesis.

Zajonc [62], elaborating on his earlier work, suggested that social facilitation effects are a product of uncertainty. Because another presence implies likely interaction, a person must be constantly prepared to react and respond to any changes in the social environment. Since being called upon to justify one’s actions to another (accountability) is a possible, albeit uncertain, outcome of interaction, one may feel the need to be prepared to respond. In this manner, the mere presence of another increases accountability and decreases intention to violate social norms.

Another alternative theory is that of self-awareness [60]. Wicklund defines self-awareness as “a state in which the person takes himself to be an object” [60, p. 234]. The presence of an observer can cause one to view oneself as an object being observed. This view prompts a person to compare their actual self to an idealized self, and, upon realizing a discrepancy, motivates them to increase performance [15]. Similarly, Schlenker [44] suggests that people generally try to make the best possible impression and have a good appearance to others. Therefore, an observer motivates another to present their best self. In an organization, an ideal self follows policies and norms, thus the mere presence of another motivates a person to achieve that ideal.

Finally, and perhaps most appropriately for our hypothesis, the mere presence of another may inhibit socially undesirable behavior. Several experiments have shown that in the presence of an observer a person will suppress behaviors that are
viewed as socially unacceptable or that could invite disapproval [30, 4].

But how do these theories fare in the digital realm? Are similar effects observed when physical presence is replaced by an electronic substitute? In Guerin’s review of mere presence effects [23] he concludes that evidence exists for social facilitation effects resulting from the passive presence of another, especially when the observer’s behavior cannot be watched. Bond and Titus [5] found that others who are imperceptible produce social facilitation effects and that they may have greater impact on a person than others who can be seen.

The concept of mere presence lends itself quite well to information systems. Social networking sites, online communication systems, and collaboration suites (and other systems) often have features enabling a user to detect the presence of another individual who is using the system concurrently. This presence, termed an “electronic presence” [1, 22], can take many forms. In a communication package, for example, electronic presence could occur by alerting a user that a contact has becoming available online. In collaboration suites, an electronic presence could be signified by a notice that work is being performed on a shared file or that a supervisor is reviewing one’s work. In any case, this concept is not foreign to systems users. Thus, we propose our final hypothesis:

H4: Awareness of another’s electronic presence will reduce intention to violate the access policy.

3. Methodology

3.1. The Scenario Method

To test our hypotheses, a factorial survey method was used [39, 26]. The factorial survey method is a specialized form of the scenario or 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” [59, p. 127-128].

The scenario method is useful to study access policy violations for several reasons. First, scenarios can incorporate situational details thought to be important in decisions to behave unethically [27]. By using a scenario approach, we can describe different system features that theorize will manipulate perceptions of accountability.

Second, scenarios can enhance the realism of decision-making situations by providing contextual detail while simultaneously ensuring that these details are uniform across respondents [2]. This allows us to describe access policy violations in situ, in the contexts in which they commonly occur.

Third, scenarios afford an indirect way of measuring intention to commit unethical behavior, which is difficult to measure directly [59]. For this reason, the scenario method is frequently used in criminological and business ethics research [35, 32]. Similarly, IS scholars have frequently used the scenario method to study IS policy violations and computer abuse [51].

3.2. The Factorial Survey Method

The factorial survey is a specialized form of the scenario method in which textual 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 [39, 26].

Like experiments, factorial surveys are constructed by designing “dimensions” (or experimental factors) of theoretical interest. In turn, each dimension comprises several “levels” (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 (i.e., a Cartesian product). The full factorial ensures that the levels are orthogonal, with correlations at or near zero, thus overcoming the problem of multicollinearity. Orthogonality is useful to test our hypotheses because we can clearly distinguish the different effects of our system manipulations. Using a traditional survey, it would be difficult to impossible to eliminate multicollinearity between our manipulations [40].

Like traditional surveys, factorial surveys adopt the technique of statistical random sampling. From the population of the full factorial described previously, a random sample of vignettes (called a pack) are obtained, which typically contain between 10 and 60 vignettes each [26]. Each survey respondent receives his or her own pack and rates an intention for each vignette contained in the pack. From the sample of all vignettes rated, estimates are obtained of the dimensions in the population of the full factorial.

In this way, estimates for a variety of factors can be obtained. Traditional experimental designs can only support a factorial of only a few dimensions with a few levels each before becoming impracticably complex. However, factorial surveys do not share this limitation. Because random sampling is used, a large number of factors and levels may be used to create a factorial of hundreds, thousands, or even millions of unique
vignette combinations [26]. This provides a rich set of factors that more closely approximate the real world.

3.3. Design of the Factorial Survey

To create a factorial survey to test our hypotheses, we first developed three scenarios that described situations common for access policy violations. The scenarios were validated for realism using two system managers and three users of a financial system with broad access rights given to its users. An example scenario is given below of an access policy violation in a university context (Table 1):

**Table 1. Example Scenario**

Each respondent received one of the three scenarios at random. In addition, the explicit statement that the scenario described an access policy violation (e.g., “Gary believes doing so may be a violation of university policy”) was also randomly varied. Some respondents received this statement in the scenario and others did not. This allowed us to examine the effect of respondent’s knowing an access policy violation was involved.

Next, we developed four system feature dimensions corresponding to the effects of (1) identifiability, (2) evaluation expectation, (3) evaluation apprehension, and (4) social presence. Each of these four dimensions had two levels each: either the system feature was described in the scenario or it was not. Together, these dimensions and levels yielded a factorial of 16 unique combinations (2x2x2x2). These dimensions and levels are summarized in Table 2.

Next, a short vignette describing a system profile was created by randomly selecting one of the 16 possible configurations of the textual elements in Table 2. This vignette represented a system profile for the user. The order in which the accountability manipulations (e.g., “unique user account”, “user activity recorded”) appeared in the vignette was also randomized to remove ordering effects.

3.4. Pretest

The instrument was pretested [6] using a sample of 102 accounting students in three sections of an accounting information systems course. Based on feedback on the pretest, the instrument was further clarified and refined.

3.5. Primary Data Collection

The primary sample consisted of 96 Information Systems majors in two sections of a course on information systems business processes and internal control. Thus, the subjects were familiar with the topic of IS security policies and computer abuse. Approximately 90 percent of participants were male, and the average age was 23 (standard deviation of 1.7).

Although use of student samples has been criticized for weak generalizability [20], business students are likely to become employees faced with access policy issues in the future [38]. Further, when the purpose of an experiment is to test theory, convenience samples can effectively falsify whether a theory is applicable to a larger population [7]. Moreover, homogeneity of a sub-sample provides a more severe test of theory by reducing statistical error that could obfuscate systematic violations of theory [8]. For these reasons, the sample is believed sufficient to test the theoretical hypotheses.

Each participant received a packet containing experimental instructions and one of the three scenarios (see Table 1). After reading the scenario, each participant was presented with 10 vignettes representing different system profiles (see Table 2). After reading each system profile, the respondent rated his or her intention (on a scale of 0 to 10) of behaving as the scenario character did given the features described in the system profile.

As is typical with factorial survey designs, the level of analysis was not the participant, but the vignette [26]. Thus, the final sample consisted of 960 observations (96 participants rating 10 vignettes each).
Table 2. Vignette Dimensions and Levels

<table>
<thead>
<tr>
<th>Accountability Dimension</th>
<th>Vignette Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unique user account?</strong> (Identifiability)</td>
<td>No. Users can use the system without logging in because all users share the same user ID.</td>
</tr>
<tr>
<td></td>
<td>Yes. Users sign into the system using a unique user ID. The welcome screen displays the user's actual full name.</td>
</tr>
<tr>
<td><strong>User activity recorded?</strong> (Awareness of logging)</td>
<td>No. There is no indication that activities in the system are recorded.</td>
</tr>
<tr>
<td></td>
<td>Yes. The login screen warns that the user's activities in the system will be recorded. Users can click to view a history of all their activity in the system. Additionally, when a user is about to perform an action in the system, a notification message warns that the current action will be logged with the user ID.</td>
</tr>
<tr>
<td><strong>Audits of log performed?</strong> (Evaluation apprehension)</td>
<td>No. There is no indication that audits of user activity will be performed.</td>
</tr>
<tr>
<td></td>
<td>Yes. All user activity in the system is comprehensively audited, according to a warning on the login screen.</td>
</tr>
<tr>
<td><strong>See other users?</strong> (Electronic presence)</td>
<td>No. The user can't see what other users are doing in the system.</td>
</tr>
<tr>
<td></td>
<td>Yes. The system is set up so that you can see what any other user is doing and they can see what you're doing without any notification.</td>
</tr>
</tbody>
</table>

4. Analysis

The dependent variable for the analysis was the participant’s reported intention of violating the access policy as the scenario character did. The four system features described in Table 2 served as predictors and were analyzed as categorical variables.

Although ordinary least squares (OLS) regression would appear to be the appropriate means of analysis, the fact that each respondent rated multiple vignettes meant observations were not independent [34]. Unobserved differences (i.e., heterogeneity) in respondents constituted a fixed individual effect that biased the vignette ratings for each respondent [21]. Because OLS does not handle mixed models of fixed and random effects, an alternative means of analysis was deemed appropriate [33, 34].

To control for control for the individual effect, we selected the SAS PROC MIXED procedure [43, 50], a generalized form of the standard linear model that allows for both fixed and random effects [31]. In contrast to OLS, the PROC MIXED procedure utilizes maximum likelihood estimations [43].

Before proceeding with the analysis, the data was examined to identify individuals who reported a zero probability of intention to violate the access policy for all 10 system profiles, effectively self-censoring their responses to zero [33]. Because these individuals cannot be made to violate the access policy any less through accountability mechanisms, these individuals were removed from the sample. Of the 96 participants in the sample, 15 were removed, leaving a sample of 81. Thus, the final sample size was 810 observations (81 participants with 10 vignettes each).

4.2. Control Variables

Five control variables were used in the analysis: (1) scenario type received, (2) whether a policy violation was explicitly stated in the scenario, (3) respondents’ reported perceived realism of the scenario, (4) respondent’s gender, and (5) respondent’s age. None of these effects were significant. The average reported realism for the scenarios was 8.1 (standard deviation of 1.7) on a 0 to 10 scale, indicating that respondents believed the scenarios were significant.

4.3. Model Test

A test of the model showed that all hypotheses were significantly supported (see Table 3). In addition, the size of each effect was calculated as the difference in the mean of the dependent variable with the effect present (a variable value of 1) or not (a value of 0). This difference was then divided by 10 (the maximum scale value) to obtain a percentage decrease in the dependent variable. Following Cohen [9], effect sizes of .02, .15, and .35, are considered respectively small, medium, and large. By this standard, the sizes of all effects can be considered small-to-medium. However, the accumulative effect for the four system design features in combination decreased intention to violate
Table 3. Results of Hypothesis Testing

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Effect</th>
<th>F-Value</th>
<th>Effect size</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Identifiability</td>
<td>31.18***</td>
<td>7.6 %</td>
<td>Yes</td>
</tr>
<tr>
<td>H2</td>
<td>Awareness of Logging</td>
<td>41.58***</td>
<td>8.5 %</td>
<td>Yes</td>
</tr>
<tr>
<td>H3</td>
<td>Audit</td>
<td>35.27***</td>
<td>7.9 %</td>
<td>Yes</td>
</tr>
<tr>
<td>H4</td>
<td>Electronic Presence</td>
<td>9.15**</td>
<td>4.1 %</td>
<td>Yes</td>
</tr>
</tbody>
</table>

N.B. *** = p < .001; ** p < .005

the access policy by 25 percent, a medium-to-large effect.

Finally, for exploratory purposes interaction effects were tested to see if combinations of accountability system design features were effective in decreasing intention to violate the access policy. The only significant interaction found was between logging and awareness of other users (F = 4.81, p < .05). The interaction had an effect size of 13 percent approximately a medium-sized effect.

5. Discussion

The results of this analysis provide several contributions. First, this study breaks new ground by applying accountability theory to the field of Information Systems. Although accountability has received substantial attention in the field of Psychology [29], to our knowledge its effects on computer abuse has not been examined. Moreover, we provided a theoretical model that showed how subconstructs of accountability—namely identifiability, evaluation expectation, evaluation apprehension, and social presence—can each affect intention to violated the access policy.

Second, the empirical test of our model found that design features of an information system can be manipulated to increase perceptions of accountability and thereby deter access policy violations. All four of our hypothesized accountability effects significantly decreased intention to violate the access policy. In addition, when used in combination, we found that the four accountability design features decreased intention by more than 25 percent.

Third, we provide practitioners with empirical evidence that accountability mechanisms can be a useful alternative to the principle of least privilege in preventing violations of access policy. In low-to-medium risk situations, our results indicate that access policy violations can be decreased simply by manipulating design features of the system. By increasing accountability within systems, practitioners may be able to ease access policy restrictions of its users, enabling greater efficiency and flexibility of system users.

6. Limitations and Next Steps

This study has several limitations. First, although support for four different forms of accountability design features were found, there may be other design features that can increase accountability perceptions among users and deter computer abuse. Further research is needed to identify other relevant accountability factors.

Second, this study examined intentions using hypothetical scenarios rather than an actual behavior within a real system. Although computer abuses, like other forms of socially undesirable behavior are difficult to measure directly [59], a field study of an actual system in use would provide additional insights.

Third, our study used students to test our theoretical model. Although this data collection choice provided a more stringent test of the theory through increased homogeneity [8], it is unclear how well these results will generalize to other contexts. Future research should examine how accountability effects using a professional sample.

7. Conclusion

The results of this study show the potential of accountability mechanisms to deter access policy violations in systems granting broad access privileges. Thus, in instances where the principle of least privilege cannot be strictly applied, or for reasons of practicality may be undesirable to do so, accountability mechanisms may provide a practical alternative.

8. References

[36] K. Price, "Decision responsibility, task responsibility, identifiability, and social loafing".


Table 4. Instrument Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Employee</th>
<th>Access to System</th>
<th>Access to Records</th>
<th>Action taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gary is a university employee with access to a student financial records system. He is approached by a supervisor of a computer support department who has noticed that some office equipment has gone missing.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td>In looking over purchase reports involving the department purchase card, the supervisor discovered that certain goods purchased are no longer in the office. Any student employee can check out the purchase card to use it to run errands to the bookstore, but it appears one student has had more discrepancies than others.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td>The supervisor thinks that a student employee is returning these items without a receipt in order to get credit on a signature card. He asks Gary to access this student’s record in the financial accounts system in order to get things straightened out.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td><strong>Although Gary believes doing so may be a violation of university policy</strong>, he accesses the student employee’s record.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td>Eric is a university employee with access to a student financial records system. He is approached by a reporter from a local newspaper who is writing an article about student school expenses.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td>The reporter says he has general information about tuition and housing costs, published by the university, but he is interested in diving a little deeper. He asks Eric to give him some reports about loans, scholarships, and general account purchases made by students. He says he doesn’t need any names or student ID’s, just the numbers.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td><strong>Although Eric believes doing so may be a violation of university policy</strong>, he looks up several records and provides the information to the reporter.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td>Charlene is a university employee with access to a student financial records system. She is approached by a friend who has a son attending college who has been living independently for a few years.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td>The friend has asked her son a few times about his financial situation but he has been repeatedly vague. The friend is concerned that he is going too much into debt to pay for his education. She asks Charlene to look up his financial aid situation to see if her concern is founded.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
<tr>
<td><strong>Although Charlene believes doing so may be a violation of university policy</strong>, she looks up the financial record of the friend’s son.</td>
<td>Employee</td>
<td>Access</td>
<td>Access</td>
<td>Access</td>
</tr>
</tbody>
</table>