AIS Transactions on Human-Computer Interaction

Volume 8 | Issue 4 Article 3

12-2016

Job Applicants' Information Privacy Protection Responses: Using Social Media for Candidate Screening

John R. Drake
East Carolina University, drakejo@ecu.edu

Dianne Hall
Auburn University, halldia@auburn.edu

J. Bret Becton
University of Southern Mississippi, Bret.Becton@usm.edu

Clay Posey
The University of Alabama, cposey@culverhouse.ua.edu

Transactions on Human – Computer Interaction

Research Paper

Job Applicants' Information Privacy Protection Responses: Using Social Media for Candidate Screening

John Drake
East Carolina University
drakejo@ecu.edu

Dianne Hall
Auburn University

Bret Brecton
University of Southern Mississippi

Clay Posey
The University of Alabama

Abstract:

For human resource (HR) departments, screening job applicants is an integral role in acquiring talent. Many HR departments have begun to turn to social networks to better understand job candidates' character. Using social networks as a screening tool might provide insights not readily available from resumes or initial interviews. However, requiring access to an applicants' social networks and the private activities occurring therein—a practice currently legal in 29 U.S. states (Deschenaux, 2015)—could induce strong moral reactions from the job candidates because of a perceived loss of information privacy. Subsequently, such disclosure requests could induce job candidates to respond in a multitude of ways to protect their privacy. Given that an estimated 2.55 billion individuals will use social media worldwide by 2017 (eMarketer, 2013), the repercussions from requests for access social media environments have potentially far-reaching effects. In this research, we examine how one such disclosure request impacted six information privacy protective responses (IPPRs) (Son & Kim, 2008) based on the job candidates' perceived moral judgment and the perceived moral intensity of the HR disclosure request. These responses occurred when we asked respondents to provide personal login information during a hypothetical interview. By modeling data derived from a sample of 250 participants in PLS-SEM, we found that the five IPPRs (i.e., refusal, negative word of mouth, complaining to friends, complaining to the company, and complaining to third parties) were all significant responses when one judged the request to be immoral and perceived the moral intensity concept of immediate harm. The amount of variance explained by these five IPPRs ranged from 17.7 percent to 38.7 percent, which indicates a solid initial foundation from which future research can expand on this HR issue. Implications for academia and practice are discussed.

Keywords: Social Media, Screening Applicants, Information Privacy

The manuscript was received 12/04/2015 and was with the authors 5 months for 2 revisions.

1 Introduction

For human resource (HR) departments, screening job applicants is an integral part in acquiring talent. While resumes and applications provide much factual and verifiable information such as educational achievements, certifications, licenses, experience, and so on, employers also use them to infer other characteristics such as personality, intelligence, leadership, and work ethic (Cable & Gilovich, 1998; Cole, Feild, Giles, & Harris, 2009). They then use these inferences to assess prospect employability (Brown & Campion, 1994; Cole, Feild, & Giles, 2003; Cole, Rubin, Feild, & Giles, 2007).

To complement traditional resumes and formal applications, employers also use online social networks—which we refer to simply as social networks here—to enhance their hiring inferences (Davis, 2007; Grasz, 2009; Kasper, 2015; Smith, 2012). This practice appears to be ubiquitous among employers. Approximately 93 percent of recruiters use or plan to used social media during the hiring process, and 55 percent have reconsidered applicants based on content found on their social media profiles (Jobvite, 2015). By examining these networks, employers attempt to compile a more comprehensive profile of applicants than would be available otherwise, especially as it relates to individuals' personalities (Kluemper & Rosen, 2009; Kluemper, Rosen, & Mossholder, 2012). Additionally, many employers approach screening applicants using social networks as an additional means of assessing "fit" with the organization or identifying "red flags" (Grasz, 2009). These "red flags" might include social network content about applicants' use of alcohol and illegal drugs, profanity, and engagement in sexually explicit behavior (Kasper, 2015). Employers often use such information to eliminate applicants from further consideration in the hiring process (Davis, 2007). In fact, 89 percent of HR professionals indicated they would be less likely to hire a candidate whose social media profile (SMP) showed evidence of "unprofessional behavior" (Grasz, 2009).

Given that individuals willingly disclose personal information in online contexts for a variety of reasons (Posey, Lowry, Roberts, & Ellis, 2010), HR representatives aim to discover personality related information about applications' suitability and fit. HR departments are increasingly turning to social networks for this information—sometimes even requesting applicants' login information (O'Dell, 2012). However, requiring access to applicants' social networks and the activities occurring therein—a practice currently legal in 29 U.S. states (Deschenaux, 2015)—will likely induce strong moral reactions in job candidates due to a potential loss of personal privacy (Black, Stone, & Johnson, 2015). Several scholars have urged caution about using social network information for screening job applicants because of these perceived privacy violations (Clark & Roberts, 2010; Davison, Maraist, & Bing, 2011; Drake, 2016; Lucero, Allen, & Elzweig, 2013; Schmidt & O'Connor, 2015), while managers argue that one needs to use social network information as a pre-employment screen to protect employers from hiring unfit applicants (Clark & Roberts, 2010). Given that two-thirds of the world's population maintains some form of social media presence (Corcoran, Elliot, Bernoff, Pflaum, & Bowen, 2009) and 71 percent of Internet users are on Facebook (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015), these HR practices have global implications for 1) how employers and associated HR departments use social networks in their vetting processes and 2) how job applicants react to employers' requests to access their social network profiles and view the activities therein. Even if many HR departments in the US have avoided requesting login information in job screening, social networking technology is evolving so quickly that privacy expectations are still in flux. By understanding the consequences of ethically questionable practices with today's privacy expectations, HR professionals can better understand how future practices might be perceived and acted on.

Unfortunately, research concerning these important issues lags behind practice. Although in its infancy, research on using social network information in employee selection has revealed some interesting findings. Early research that focused on applicant reactions to computer-based employment testing and internet recruiting (Anderson, 2003; Rozelle & Landis, 2002) suggests that applicants have negative perceptions of or reactions to Internet- and computer-based recruitment and selection. More recently, scholars have begun to examine social networks as part of the selection process. Research has shown that social network information does not relate to supervisor ratings of performance, turnover intentions, or actual turnover nor does it contribute to the prediction of cognitive ability, self-efficacy, or personality (van Iddenkinge, Lanivich, Roth, & Junco, 2013). Furthermore, applicants tend to oppose the use of social network information for employment decisions (Drouin, O'Connor, Schmidt, & Miller, 2015). For example, Brown and Vaughn (2011) suggest that selection procedure characteristics impact applicant's perceptions of fairness, and online background checks may violate individuals' sense of privacy.

Applicants' potential reactions are rooted in their motivations and beliefs as the theory of reasoned action and the theory of planned behavior posit (Madden, Ellen, & Ajzen, 1992). In particular, various ethical, cultural, and organizational norms affect individuals' expectations of information privacy (Loch & Conger, 1996; Mizutami, Dorsey, & Moor, 2004; Smith, Dinev, & Xu, 2011). Of these three factors, little research has examined the impact of ethical issues on human computer interaction (HCI) (Zhang & Li, 2005). Privacy research in particular has focused more on concerns for privacy and paid little attention to individuals' ethical decision making and actions to protect privacy (Belanger & Crossler, 2011; Smith et al., 2011) in spite of the fact that privacy violations are considered immoral and sometimes illegal (Moore, 2010). One exception is the privacy model (Black et al., 2015) in which norms about privacy and ethical beliefs about violations therein affect job candidates' behavior. However, little empirical evidence has validated the model. Furthermore, few research efforts have specifically investigated the use of social media in making employment decisions (Roth, Bobko, Van Iddenkinge, & Thatcher, 2013).

Given these opportunities, we explore job candidates' potential reactions when confronted with a request to provide social network login information to a potential employer's HR department during the vetting process. When one views social networks as part of a socio-technical system, the technology enables and constrains behavior by and between individuals in that system. The use of social networks for job screening and subsequent changes in job candidates' usage behavior both directly and indirectly fall in the HCI tradition when exploring the social and organizational context surrounding social network usage. Because social networks enable interactions between individuals in unique ways, HCI studies about social networks can include not only the singular interaction between one individual and the technology but also the relational interaction between individuals including the sharing of private information.

Because information privacy is an ethical issue (Mason, 1986), we frame our discussion in terms of the issue-contingent model of ethical decision making (Jones, 1991). This model is appropriate since we examine privacy for a specific issue, and we know privacy to depend on context (Smith et al., 2011). Also, the model acknowledges that not everyone recognizes and judges the morality of the issue in a similar fashion, which is important because individuals have free will in ethical decision making (Smith, 2000) and use a diverse set of ethical perspectives when making those decisions (Drake, Hall, & Lang, 2009; Reidenbach & Robin, 1990). Therefore, we address two research questions in this paper:

RQ1: Do individual ethical decisions and the perceived intensity of the moral dilemma affect an applicant's intentions to protect information privacy of social network accounts when confronted with requests for login information from potential employers?

RQ2: Which of the information privacy protective responses do the ethical judgments and perceived intensity of the login information requests most influence?

This paper proceeds as follows. In Section 2, we detail the theoretic foundations for our model. We start the traditional ethical decision making models, explore how moral intensity impacts that model, and consider various information privacy protective responses that job candidates might employ. From that foundation, we develop hypotheses in Section 3 and explain our methodology for testing the hypotheses in Section 4. In Section 5, we present the results and, in Section 6, discuss implications based on these findings.

2 Background

According to the traditional ethical decision making model, individuals go through a series of steps when deciding how to act in moral contexts (Jones, 1991; Rest, Narvaez, Bebeau, & Thoma, 1999; Trevino, 1986). This process begins with the awareness and recognition that an issue belongs to the realm of ethics. Decision makers' knowledge, ethical perspectives, and ingrained moral principles bound how they recognize an issue as something of ethical importance (Miner & Petocz, 2003; Woiceshyn, 2011). Assuming that the individual believes an issue is of moral consequence, one then has to judge whether the issue is moral or immoral. Based on the response, the individual develops intentions on how to deal with the ethical issue. These intentions generally predict the individual's subsequent actions.

However, individuals who make moral judgments may use a wide variety of sometimes contradictory ethical beliefs (Evans, 2008) or compartmentalize ethical beliefs based on the issue and context (McDonald & Pak, 1996). To overcome these limitations, the issue-contingent model of ethical decision making further suggests that, when describing behavior, an issue's moral intensity and various personal, environmental, organizational, and cultural beliefs influence each of the above steps (Jones, 1991). As

Jones (1991) describes, moral intensity represents the saliency of an issue to an individual. The more salient the issue, the more likely individuals are to recognize, judge, intend to act, and act to mitigate the issue. Because of the ethical implications of trying to test the actual behavior of privacy violations, we confine our study to recognition, judgment, and intention as Figure 1 details.

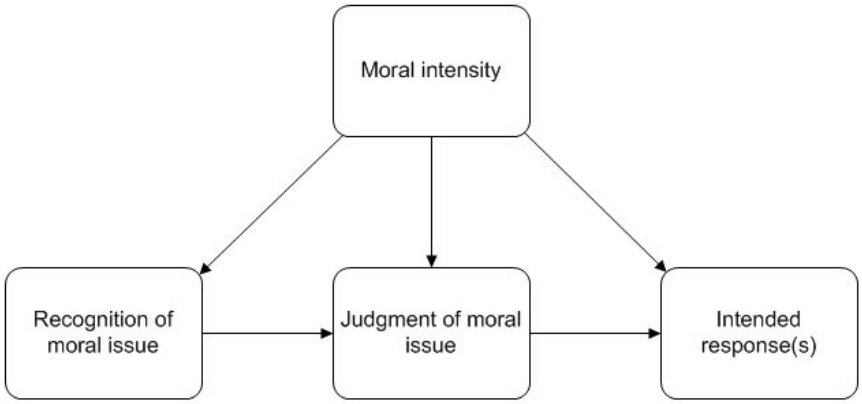

Figure 1. High Level Theoretical Model of Ethical Decision Making

2.1 Moral Intensity

As a moral issue gains salience to an individual, it impacts the individual's recognition, judgments, and intentions (Jones, 1991). Moreover, moral intensity comprises six subfactors: magnitude of consequence, proximity, social consensus, probability of effect, temporal immediacy, and concentration of effect (Jones, 1991). Various empirical studies have confirmed the salience of each of these factors and found that each generally impacts how individuals recognize a moral issue, judge a moral issue, and intend to act on a moral issue (May & Pauli, 2002; Singhapakdi, Vitell, & Kraft, 1996; Valentine & Fleischman, 2006). When operationalizing these subconstructs, Barnett (2001) found that he could collapse the six factors into four factors: social consensus, temporal immediacy, proximity, and magnitude of consequence. Social consensus represents a perception that a general agreement in the culture on the nature of the particular issue exists. The more strongly the culture agrees, the stronger the moral intensity. Temporal immediacy represents the perceived timeliness in which one expects the issue to have a harmful impact. For example, if one expects the moral transgression to have an impact after 50 years, then the moral intensity would be weaker than if one expected it to happen tomorrow. Proximity represents how similar to the decision maker the offender of the moral transgression is. The more similar the transgressor, whether in general demographics or in physical proximity, the stronger the moral intensity. Because the subject of the moral transgression in our study was the participant, proximity was not relevant, so we did not measure it. Finally, the magnitude of harmful consequences represents the size of the moral transgression's consequences. The greater the magnitude of consequences, the stronger the overall moral intensity.

2.2 Privacy Protection

Privacy represents a preferred state in which an individual is protected from intrusion, interference, and information access by unwanted others (Tavani, 2007; Tavani & Moor, 2001). Privacy is both a state of being and a value to be desired (Smith et al., 2011). Individuals value it for numerous reasons, including the ability to act without second-guessing a decision due to what others might think (Rachels, 1975), to enjoy a value without interruption or worry (Thomson, 1975), to work in solitude or absolute quiet in order to concentrate (Peikoff, 2008), and to protect knowledge of something to reduce chances of theft or exploitation (Warren & Brandeis, 1890).

Organizations, for their part, protect or fail to protect privacy through their behaviors in information releases, social exchanges, and environmental structuring (Stone & Stone, 1990). These behaviors stem from motivational forces to protect privacy throughout the organization. Various factors about the nature of the information, the physical environment, social and cultural norms, and individual characteristics guide the formation of thoughts, policies, and systems implemented in organizations to protect privacy (Stone & Stone, 1990).

In terms of communication, the person speaking must balance information privacy with the self-disclosure inevitable when communicating (Altman, 1975). By knowing the boundaries of the disclosures, individuals can make rules for managing and maintaining privacy even if those boundaries are dynamic and change over different contexts, over different technologies, and over time (Petronio, 2002). This conception of communication boundaries helps explain disclosure patterns on Facebook (Stutzman, Capra, & Thompson, 2011). It also helps explain why privacy concerns and the desire for awareness positively impact attitudes toward certain communication technologies such as instant messaging (IM) more so than other communication technologies such as blogs and social networks by (Lowry, Cao, & Everard, 2011). Each of these technologies induces boundary expectations that define how individuals choose to disclose information. When someone attempts to breach those boundaries, they threaten others' privacy.

When others threaten one's privacy, one has to maintain control over that state of privacy for their own protection. One can maintain control over their privacy via legislative, regulatory, and judicial means (Moore, 2010; Peikoff, 2008) or by personal action (Son & Kim, 2008). Because of the limited legal protection that current U.S. laws provide (Clark & Roberts, 2010), individuals often need to take personal action to maintain their privacy. For this reason, researchers have identified three broad types of personal actions that individuals use to protect their own privacy (i.e., information privacy protective responses (IPPR)): information provision, private action, and public action (Son & Kim, 2008). As it relates to our research questions, IPPR suggests a set of behavioral responses that job applicants might employ when they perceive information privacy threats from a company's requesting to access their social media accounts.

2.2.1 Information Provision

When confronted with privacy threats, job seekers can delineate how they want to deliver their personal information to the hiring company. When submitting a resume or interviewing for a position, job seekers must not only choose what information to include but also what information to exclude. When companies threaten privacy with requests for social media logins, job applicants can provision information in two ways (Jiang, Heng, & Choi, 2013): they can refuse to disclose their social media login credentials or they can misrepresent their social media activity.

Previous research has found that individuals will sometimes refuse to disclose personal information when confronted by marketers' requests for information (Malhotra, Kim, & Agarwal, 2004; Stewart & Segars, 2002). Others have found that, in online communities, perceived risk in disclosing personal information negatively affects self-disclosure (Posey et al., 2010). Omissions on resumes may be innocuous or attempts to hide personal information that shows the job candidate in an unfavorable light, such as a rapid succession of jobs or time in prison (Jones, 1984). In the context of this study, refusal refers to the intention to not disclose one's social media login credentials to a company.

While refusing to disclose information to hiring companies seems straightforward, some job seekers may purposefully misrepresent themselves. Misrepresentation on resumes, even if minor embellishments, seem to infect nearly half of all resume submissions (Bata, 2009; Kuhn, Johnson, & Miller, 2013). Even CEOs and doctors have been found to submit resumes and curriculum vitae with misrepresented information (Efrati & Lublin, 2012; Goe, Herrera, & Mower, 1998). On social media sites such as Linkedin.com, job candidates are more likely to embellish extracurricular interests and activities when their profiles are public (Guillory & Hancock, 2012). Some of these misrepresentations may be attempts to bolster the applicant's image, while others may be used to protect their privacy. Misrepresentation may even include one's claiming they have no social media presence when in fact they do (whether active or not).

2.2.2 Private Action

When individuals are about to lose control of their personal information, they can protect their information via their own action. Outside parties may not be able to view such actions, yet the actions help an individual protect personal information that may be at risk. Son and Kim (2008) identify two such private actions—removing information and participating in negative word of mouth.

Son and Kim (2008) infer that individuals remove information only from offending companies' databases, such as through opt-out procedures. However, one can conceive of removing information more broadly as applying to external databases that the offending company has access to, such as found on social media platforms. In our study, we refer to removing information as cleansing social media accounts to help

protect the job seekers' personal information if they comply with the HR request. Such removal can range from individual pieces of information (e.g., birthdate, religious affiliation, private messages, offensive pictures) to entire accounts.

Job seekers may concurrently speak confidentially with friends and family about their negative experiences with the offending employer. Negative word-of-mouth communication can damage the offending company's reputation (Resnick, Zeckhauser, Friedman, & Kuwabara, 2000). Similar to negative word-of-mouth communication that consumers participate in, researchers have posited that word-of-mouth communication by job applicants can impact other people's attitudes and behaviors (Collins & Stevens, 2002; Van Hoye & Lievens, 2005, 2007, 2009). Furthermore, research indicates that perceived privacy invasion stemming from social media use in the hiring process results in negative applicant reactions (Clark & Roberts, 2010; Cole, 2011; Davison et al., 2011). Additionally, applicant reactions to the use of social media in the hiring process can have important consequences related to factors that influence willingness to accept job offers. For example, Siebert, Downes, and Christopher (2012) found that requesting access to applicants' private information decreased attraction to the organization.

2.2.3 Public Action

Finally, social media users dissatisfied with the employer's request for social media login credentials may also engage in public action as a form of recourse or to seek a remedy. Son and Kim (2008) identify two such public actions: complain to the company and complain indirectly to a third party. Given the nature of interviews, individuals are not likely to complain about the requesting during them. Instead, we focus on complaints to companies' executives. Indirectly complaining to a third party may include contacting the media or local politicians to seek redress.

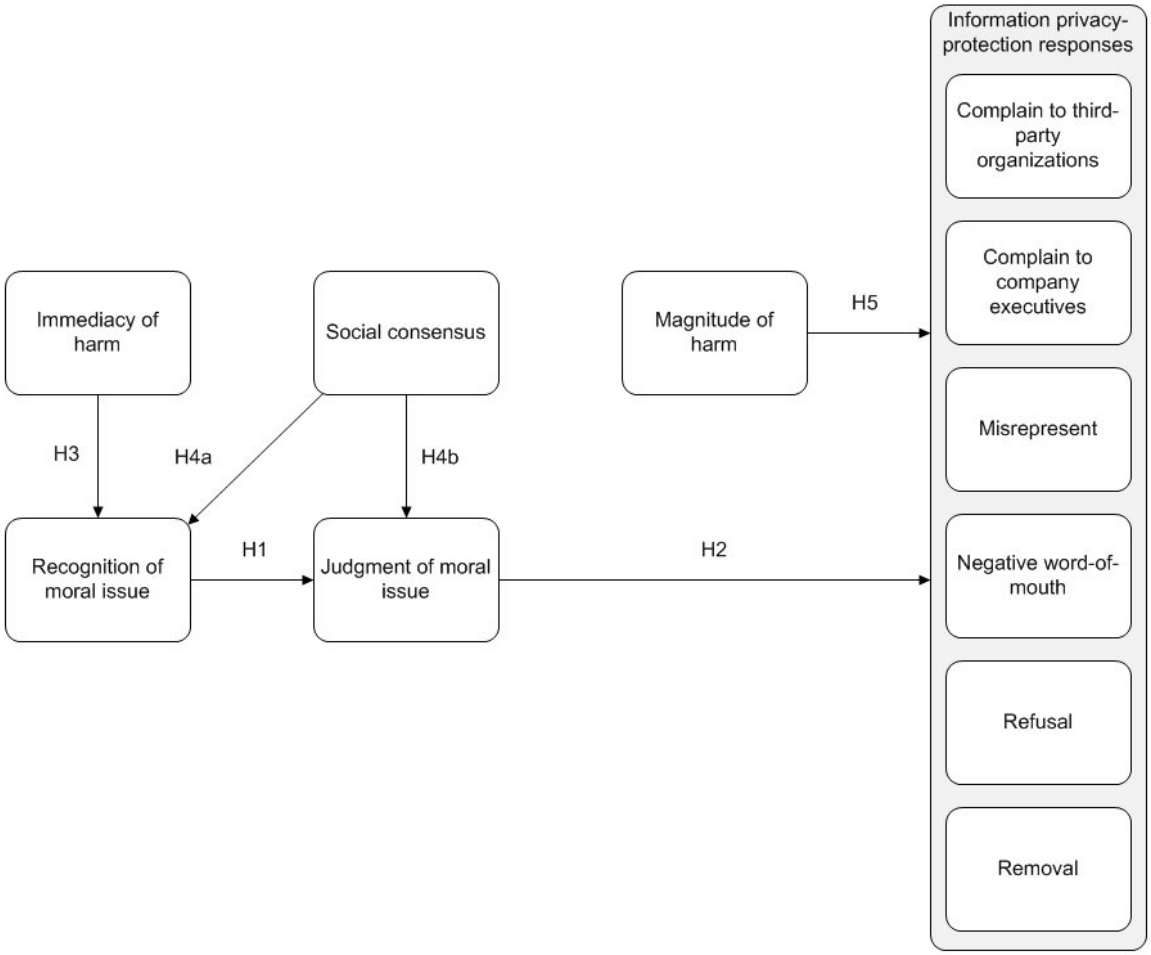

Figure 2. Extended Ethical Decision Making Model

3 Hypotheses Development

Figure 2 summarizes the model and hypotheses we propose. Many studies have empirically validated the ethical decision making model that Jones, Rest, Trevino, and others (Jones, 1991; Rest, 1986; Trevino, 1986) propose (Lehnert, Park, & Singh, 2014; Loe, Ferrell, & Mansfield, 2000; O'Fallon & Butterfield, 2005). Across many contexts, one's recognizing that an issue is morally charged positively impacts how one judges the issue. For example, Featherman and Pavlou (2003) found that perceived risk, which included perceived risk to privacy, had a negative impact on perceived usefulness of e-billing systems and a negative impact on adoption intentions, which suggests that negative evaluations of privacy violations might impact how one judged a system. Following that line of research, we suspect that individuals will more likely judge a request for login information as immoral if they recognize it as a moral issue.

H1: Job applications are more likely judge a request for login information as immoral if they recognize it as a moral issue

Individuals often form moral judgments quickly based on principles formed through integrating prior observations (Woiceshyn, 2011). These moral judgments activate emotional responses that motivate the judger to action. That motivation translates into intentions.

Just as recognizing an issue as moral impacts subsequent judgment, previous research has empirically confirmed that the moral judgment impacts one's intention to act on that judgment (May & Pauli, 2002). However, for our purposes here, we are not interested in how moral judgment can determine an individual's intention to engage in a single behavior; rather, we examine its potential to impact intentions regarding any number of the six potential IPPR responses that Son and Kim (2008) identify.

H2(a-f): Job applicants who judge a request to share social media login information as immoral are more likely to engage in information privacy protective responses.

As we discuss earlier, the more immediate an individual perceives the moral issue's harm to be, the more salience the issue will have for the individual. If sharing information now won't have a negative impact for many years down the road, then the danger appears too far in the distance and fails to register as even something worthy of significant consideration. Thus, one fails to even recognize the issue as a moral issue (Singhapakdi et al., 1996). We believe this assertion will hold true for requests for social media login information from HR departments. Conversely, as the perceived immediacy of harm increases, so will the recognition that the request is immoral.

H3: The more immediate job applicants perceive the harm from a request to share their social media login information, the more likely they are to recognize the request as a moral issue.

When referent groups surrounding an individual generally agree that a specific action is right or wrong, the individual tends to follow suit. In examining the power of social influence, Cialdini (2001) found individuals to engage in activities if they knew others in their environment were doing so too. Social consensus works in a similar way: it provides social proof that the moral issue is salient and, thereby, triggers recognition and judgment of that moral issue. Research has shown social consensus to impact moral awareness (Butterfield, Trevino, & Weaver, 2000; Singhapakdi et al., 1996) and moral judgment (May & Pauli, 2002). Likewise, we expect perceptions of social consensus to impact how strongly job applicants recognize and judge the morality of a HR request for social media login information.

H4: Job applicants who perceive that social consensus regards the request to share social media login information as immoral are more likely to 1) recognize that the request is a moral issue and 2) judge it as immoral.

Finally, the third component of moral intensity, the perceived magnitude of harm, should play a significant role in impacting intended responses to an immoral request. Rather than impacting how individuals judge the issue as moral, magnitude of harm relates more closely to intention (Schwartz, 1989). Researchers have used this argument to help explain why some e-commerce buyers use signals to evaluate sellers and intend to bid on online auctions (Drake, Hall, Cegielski, & Byrd, 2015). For mobile applications, perceived risks with disclosing location data also impact individuals' behavioral intentions in willingness-to-pay and intention-to-adopt location-based services (Keith, Babb, Lowry, Furner, & Abdullat, 2015). Further, research in HR contexts has shown that the perceived magnitude of consequence has a strong

impact on moral intent (Watley & May, 2004). For these reasons, we expect the perceived magnitude of harm to have an impact on the six intentions to protect information privacy when an individual faces requests for social media login information.

H5(a-f): The perceived magnitude of harm from a request for social media login information increases job applicants' intentions to engage in information privacy protective responses.

4 Methodology

4.1 Data Collection

We focused on job candidates as our target population; therefore, we collected data from college students who were likely searching for jobs, would be searching for jobs in the near future, or were discussing job opportunities with friends. Additionally, university students generally use social networking platforms more than the general population, which further enhances the relevance of our chosen context to the respondents. We contacted graduate students and third- and fourth-year undergraduate students from three public U.S. universities and offered them extra credit for participation. We sent out email invitations to potential participants. We used a Web-based questionnaire so that participants could take the survey in a location of their choosing, which helped to ensure the results' confidentiality. We limited survey completions by IP address so that participants could provide data only once.

We collected 250 usable (from 285) responses. We omitted 35 responses because of incompleteness, trivial responses (e.g., selecting all 1s for every response), no experience with social media, or duplicate responses (identified by IP address of the participant). As for the individuals that provided the usable responses, 50 percent were 25 years of age or younger, and 44 percent were female (see Table 1 for demographic information). In the month prior to completing the survey, over 50 percent posted something to a social networking site at least once per week. Sixty-nine percent of respondents spent more than five minutes per day on a social networking site.

We also found that the job search context was largely relevant to the study participants. In two months after they completed the survey, 64 percent expected to send a resume to a potential employer, 51 percent expected to list themselves on a job applicant website, 61 percent expected to fill out a job application form, 62 percent expected to email a prospective employer, and 60 percent expected to have a job interview.

Table 1. Demographic Information

Age (in years)	18-25	13.7%
	26-30	36.1%
	31-35	24.1%
	35-40	17.7%
	41-50	6.0%
	51-60	1.6%
	61+	0.0%
Education	High school	1.2%
	Some undergraduate	25.8%
	Bachelor's degree	13.3%
	Some graduate work	42.7%
	Master's degree	14.9%
	Doctorate's degree	2.0%
Gender	Male	55.4%
	Female	43.8%

4.2 Measurement

We carefully crafted the survey instructions to avoid ethically charged terms such as dishonest, unethical, misdeeds, and so on. The title of the survey (i.e., "Attitudes toward social networking privacy") and the stated purpose (i.e., "to gain a better understanding of individual perspectives toward social media privacy concerns) used neutral wording to avoid priming the ethical decision making questions. The instructions also did not mention any of the privacy protective responses.

We adapted all constructs in this study from existing measures (see Appendix A). The dependent variables comprised the six information privacy-protective responses that Son and Kim (2008) identify. Consistent with the original instrument, we measured each of the constructs with three items: how likely/unlikely, how probable/not probable, and how possible/impossible (on a seven-point Likert scale). We adapted moral intensity measures from Barnett (2001). For each construct, we used three items measured on a seven-point Likert scale. Moral recognition and judgment of moral issues came from Reynolds (2006). Moral recognition was a two-item construct, while moral judgment used four items.

The scenario comprised a vignette that established an ethical quandary between two potential values: gainful employment and personal privacy. We designed the scenario to mimic a real news story about employers' asking job applicants for their Facebook login and password (O'Dell, 2012). We chose this story because it could potentially cause a strong moral reaction necessary for the ethical decision making model to have validity. The vignette also ensured relevance of the study to the real world. We evaluated the face validity of the vignette with a pilot study of 65 participants (MBA students). We asked these participants of their impression of the survey. All of them found the vignette plausible. While they seemed to answer the questions appropriately, some voiced concerns that the wording was confusing. As such, we reworded the vignette to avoid confusion in the full sample. The vignette read as follows:

> *Imagine you are interviewing with an organization for a position that perfectly fits your skills, location, salary, and working conditions. During the interview, the interviewer informs you that due to problems in the past, they now request all job applicants to share their username and password to all social media accounts to help establish the character of the applicants. The interviewer indicates that they will review these accounts over the coming two weeks and then make their decision.*

4.3 Controls

Research has established that age and education affect ethical decisions (Ruegger & King, 1992). We used these two factors as controls on the dependent variables. Likewise, research has shown concern for privacy to impact intentions when something threatens individuals' privacy (Dinev & Hart, 2005; Stewart & Segars, 2002). In particular, concern for privacy increases some IPPR intentions (Son & Kim, 2008). We used a concern for privacy instrument to control for this effect and allowed it to covary with the dependent variables.

5 Analysis and Results

We performed partial least squares analysis using SmartPLS version 3.0. We chose component-based SEM rather than covariance-based SEM because our study is an initial examination into IPPR responses and the factors that most readily predict these responses in the HR context. We measured all constructs reflectively; hence, traditional means of assessing construct validity were appropriate (Chin, 2010; Gefen & Straub, 2005). We calculated internal consistencies with both composite reliability and Cronbach's alpha for each latent construct and found all constructs were greater than 0.70, which indicates sufficient internal consistencies (Table 2). We established convergent validity by calculating t-values of the outer model loading of all items (Gefen & Straub, 2005), which also extended beyond the 0.70 heuristic.

We established discriminant validity by comparing the inter-construct correlations with the square root of the average variance extracted (AVE) scores of each construct considered in the correlations (Fornell & Larcker, 1981; Gefen & Straub, 2005). All correlations were less than the square root of AVE for each construct, which indicates sufficient discriminant validity. We also found that all AVEs were above 0.50 heuristic, which suggests that the principle components captured construct related variance rather than error variance. To further confirm validity, we performed a confirmatory factor analysis (CFA). In the initial CFA, all items loaded on their respective constructs with a highly significant t-value ($p < 0.001$).

To check for common method bias, we performed Harman's single-factor test (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003) and examined the correlation matrix of the constructs to determine if any correlations were above 0.90 (Pavlou, Liang, & Xue, 2007). In the first test, the model fit was not significant, which suggests that no single factor explained the results. In the second test, the highest correlation was 0.73 (results > 0.90 suggest a common bias in the data). Because we did not find those high correlations, common method bias is unlikely.

Given our validity checks, we tested the path model. We calculated the significance of the path estimates using a bootstrap with 200 re-samples. Table 3 summarizes the test of hypotheses, controls, and variance explained as reported by R^2 values.

Table 1. Internal Consistencies and Interconstruct Correlations

	Mean (SD)	α	CR	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Age	N/A	N/A	N/A	N/A													
2. Concern for Information Privacy	5.70 (1.17)	0.87	0.91	0.138	**0.840**												
3. Education	N/A	N/A	N/A	0.360	0.131	N/A											
4. IPPR: Complain to Exec	4.33 (1.97)	0.98	0.98	0.052	0.088	0.069	**0.976**										
5. IPPR: Complain to TP	3.76 (2.00)	0.98	0.99	0.058	0.037	0.059	0.735	**0.978**									
6. IPPR: Misrepresent	2.67 (1.94)	0.98	0.99	-0.109	0.042	0.028	0.109	0.285	**0.983**								
7. IPPR: Negative WOM	5.92 (1.47)	0.95	0.97	0.021	0.153	0.183	0.312	0.203	0.102	**0.953**							
8. IPPR: Refusal	5.44 (1.61)	0.95	0.97	0.106	0.079	0.142	0.479	0.401	0.075	0.459	**0.950**						
9. IPPR: Removal	4.53 (2.08)	0.98	0.98	-0.052	0.072	-0.021	0.259	0.310	0.415	0.268	0.271	**0.976**					
10. Immediacy of harm	4.32 (1.88)	0.98	0.99	0.069	0.084	0.101	0.290	0.335	0.234	0.139	0.229	0.296	**0.983**				
11. Judge moral issue	5.67 (1.23)	0.84	0.89	0.063	0.286	0.197	0.458	0.360	0.062	0.455	0.575	0.276	0.263	**0.821**			
12. Magnitude of harm	4.19 (1.83)	0.97	0.98	0.082	0.159	0.050	0.360	0.395	0.229	0.071	0.336	0.359	0.550	0.250	**0.970**		
13. Recognize moral issue	5.88 (1.30)	0.84	0.93	0.116	0.197	0.241	0.258	0.203	0.019	0.306	0.346	0.139	0.250	0.637	0.122	**0.930**	
14. Social consensus	4.44 (1.33)	0.88	0.92	0.058	0.052	0.068	0.254	0.174	0.048	0.225	0.282	0.105	0.094	0.305	0.182	0.205	**0.895**

Note: bolded values on diagonal represent √AVEs.

The results support our hypotheses (see Table 3). Participants' recognizing a request for their social media login information as a moral issue positively impacted how negatively they judged this issue. Negative judgment of the moral issue positively impacted all information privacy protective responses except misrepresentation. Of the moral intensity hypotheses, immediacy of harm positively impacted how strongly participants recognized the request, social consensus positively impacted how strongly participants both recognized and judged this moral issue, and magnitude of harm positively impacted the probability that participants would use all of the information privacy protective responses except negative word of mouth.

Table 3. PLS-SEM Results

Information privacy-protection responses (IPPRs)	β	Complain to TP	Complain to exec	Misrepresent	Negative WOM	Refusal	Removal
Controls							
Age → IPPRs		0.038 (0.689)	0.025 (0.443)	-0.155** (2.921) *0.022*	-0.048 (0.641)	0.068 (1.351)	-0.066 (1.067)
Concern for information privacy → IPPRs		-0.106 (1.619)	-0.075 (1.174)	0.022 (0.311)	0.022 (0.387)	-0.127* (2.230) *0.023*	-0.024 (0.345)
Education → IPPRs		-0.006 (0.099)	-0.030 (0.544)	0.077 (1.114)	0.100* (1.883) *0.011*	0.004 (0.067)	-0.050 (0.772)
Hypotheses							
H1. Recognize moral issue → Judgment of moral issue	0.599*** (8.248) *0.612*						
H2: Judgment of moral issue → IPPRs		0.315*** (5.599) *0.112*	0.415*** (7.473) *0.203*	-0.006 (0.092)	0.440*** (6.412) *0.210*	0.553*** (9.592) *0.421*	0.221*** (4.354) *0.050*
H3. Immediacy of harm → Recognize moral issue	0.246*** (4.512) *0.066*						
H4a. Social consensus → Recognize moral issue	0.164** (2.737) *0.029*						
H4b. Social consensus → Judgment of moral issue	0.183** (3.089) *0.057*						
H5. Magnitude of harm → IPPRs		0.339*** (6.246) *0.141*	0.266*** (4.134) *0.091*	0.235*** (3.756) *0.055*	-0.046 (0.699)	0.210*** (3.308) *0.066*	0.316*** (4.807) *0.113*
R^2		0.248***	0.275***	0.073**	0.215***	0.382***	0.177***

Judgment of moral issue: R^2 = 0.435***, Recognize moral issue: R^2 = 0.096***
* p < .05, ** p < .01, *** p < .001
Standardized betas on top; t-stats from bootstrap in parentheses; f^2 values italicized for significant relationships.

6 Discussion

Our results suggest several implications for research in information privacy, human-computer interaction, and human resource management. Furthermore, they have implications for the organizational practice of job screening with social media accounts. We discuss these implications and the limitations of our research below.

6.1 Implications for Research

In this study, we examine how a human resource's perceived unethical request for social media access impacts job seekers' potential responses to the personal privacy threat. For example, the impact of privacy threats on social media usage can work directly through individuals' changing or removing content and indirectly because complaints and negative word of mouth lead to social, ethical, and political pressures that might impact other individuals' interactions with social media and organizations. When organizations demand job candidates disclose social media identification and authentication credentials, negative word of mouth and public actions by a job seeker might create a public backlash. These actions, in turn, will likely change how employers interact with social media as a way to screen for jobs. While information privacy is a noted ethical issue (Mason, 1986; Smith et al., 2011), we have extended existing theory by showing how privacy threats induce the ethical decision making process. In particular, our research indicates that the issue of job screening with social media information induces the ethical decision making process. Individuals' intentions to protect privacy in that context through refusing to disclose login information, removing content from social media accounts, engaging in negative word of mouth publicity, and complaining to the company executive and third parties depend on how immoral they judge the request.

In addition, we show that how morally intense the job candidate perceives the request impacts the ethical decision making process. That is, the immediacy of harm to the candidate impacts how strongly participants recognize the issue as morally salient. Social consensus—the degree to which one expects others to believe the request is immoral—impacts job seekers' recognition and judgment of the act as immoral. Furthermore, the magnitude of harm from the request significantly impacts job candidates' intention to 1) refuse to disclose their login information, 2) misrepresent themselves, 3) remove content from their social media accounts, 4) complain to company executives, and 5) complain to third parties.

Of the two information provision protective responses (i.e., refusal and misrepresentation), there seemed to be little perceptual overlap, with a very small correlation between each. Misrepresentation, similar to prior research (Jiang et al., 2013), was the most weakly predicted intention (R^2 = 0.073): only the magnitude of harm and the age of the participant significantly impacted it. Younger job candidates seemed more likely to misrepresent, although we note it was not a large effect (β = -0.156), and one should not see it as an indictment of the younger generation. However, refusing to disclose information was very closely linked to how one judged the moral issue. These two provisions do not appear opposite each other but more orthogonal; that is, many participants may choose one or both provisioning techniques independent of the other. While refusal seems tightly integrated with how one judges the issue, misrepresentation shows no such relationship. Given the small R^2 for misrepresentation, we need more research to investigate the causes of that choice above and beyond magnitude of harm and age of the job candidates. For example, previous research found that publically available LinkedIn profiles exhibited lower levels of misrepresentation of responsibilities but higher levels of misrepresentation of interests than private LinkedIn profiles or traditional resumes (Guillory & Hancock, 2012). Thus, we need to further examine the driving forces behind misrepresentation and its moderating contexts.

The two private actions, negative word of mouth and removal, showed only a modest correlation with each other. In the model, the judgment of the issue and the education level of the participant best predicated negative word of mouth. The perceived magnitude of harm, however, seemed not to impact the choice to spread negative word of mouth to friends and family. We may have obtained this result because perceptions of injustice, as the judgment of immorality may be, seem to elicit feelings of anger and outrage (Mikula, Scherer, & Athenstaedt, 1998). Experiences of anger, frustration, and irritation seem to relate to NWOM for goals of venting and taking revenge (Wetzer, Zeelenberg, & Pieters, 2007). Such venting or revenge NWOM may follow the judgment regardless of the perceived magnitude of harm.

The two public actions (i.e., complaining to third parties and complaining to executives) exhibited a high correlation and shared similar outcomes in the model. Considering how closely these two actions relate, there is likely a similar element underlying the motivation besides protecting privacy. By making it public,

each may be attempting to change the process either directly by complaining to the executives or indirectly through the popular press or legislative means.

While the privacy paradox suggests that concerns about privacy do not line up with self-disclosure intents and behaviors, researchers have criticized some of this literature for using overly broad definitions of privacy attitudes but narrow measures of intention and behavior (Acquisti, Brandimarte, & Loewenstein, 2015). Others have argued that the privacy paradox emerges because people have not thought deeply or carefully about information privacy, so their responses tend to be generalized rather than specific (Baek, 2014). In our study, we used concerns for information privacy (CIP) as a control. Our findings generally confirm the privacy paradox with no significant relationship between CIP and intentions to protect information privacy with one exception. In that exception, CIP had a negative impact on refusal to disclose social media login information. The more concern a job seeker had in general for the privacy of their information, the less likely they were to refuse the request to provide social media login information to a company's HR representatives once one factors in the ethical judgment and perceived magnitude of harm. Paradoxically, CIP had a small but positive correlation with refusal to disclose. This counter-intuitive result may shed some light on the privacy paradox. As we mention previously, one can see privacy as both a state of being and a value of ethical importance (Smith et al., 2011). Concern for privacy could potentially include both aspects: concern about the current state of privacy protection and concern about the ethical implications in the loss of privacy. While the ethical implications of the request accounted for the ethical implications, we did not directly measure the current state of privacy protection. If participants viewed the current state of privacy protection to be weak, they might believe immediate action, such as refusal, to be outside of their control. They might be concerned but feel powerless to do anything about it in the moment. Future research could help clarify how concerns about privacy manifest themselves in behavior to protect that privacy. Such research could look at self-efficacy with privacy protection and environmental factors that diminish that capability.

In a privacy model of factors that impact applicants' reactions to the use of social media websites in the employment process, individual, procedural, socio-cultural, and information factors impact beliefs about ability and consequences of controlling or not controlling SNS data (Black et al., 2015). In our study, we complement this privacy model. Specifically, we embedded procedural factors in the scenario by stating advanced notice of data collection in the vignette. We also embedded the social media login information's purpose in the vignette, which we described as a background check. We also included various socio-cultural and individual factors in the survey with age, education, CIP, perceived social consensus, perceived immediacy of harm, and perceived magnitude of harm. All of these factors impacted ethical judgments and intentions to act to protect one's privacy. Our findings provide support for this model.

Lastly, we address a void in the HR literature by investigating applicant reactions to invasions of privacy in the form of requesting SNS identification and authentication credentials. As Roth et al. (2013) clearly outline, we know little about reactions to the use of social media in the hiring process and, specifically, about organizations' requiring applicants' passwords or access to their private information. Our research is among the first efforts in this area and provides important implications for practice and future research opportunities.

6.2 Implications for Practice

The practice of screening job applicants requires HR representatives to use the tools available to them to filter job candidates quickly and appropriately. Job applicants may perceive organizations that search their websites and social media sites as violating their privacy. Doing so could induce job candidates to protect their privacy through actions that could hide their information, misrepresent themselves, or induce them to start talking to others, which could negatively impact the hiring company's reputation. These actions are particularly pronounced when HR representatives request applicants' social media login information.

Of course, some situations might warrant hiring organizations to ask for social media login information, such as if the job requires using a personal social media account to act on behalf of the company. Such cases might occur when specialized marketing strategies attempt to appear less formal and more authentic. A background check is also warranted if the job entails access to extremely sensitive information (e.g., military secrets). Extensive background checks and security clearances are required for some federal jobs, which likely require access to social media accounts.

Besides possible ethical concerns, legal concerns abound as well. Negative word of mouth and complaints to third parties such as politicians could lead to heightened political sensitivity and attention.

While the scenario we used was not uniformly illegal under criminal law, social media companies could potentially file a tort for interference of contract against companies that require users to violate terms of service for a job (Drake, 2016). For example, Facebook's terms of service at one point stated that users should not share their password with anyone (Facebook, 2012). If a company requires a job applicant to disclose their password, the job applicant would have to violate Facebook's terms of service in order to comply with the request. Such a request violates the contract between Facebook and its users. While such a case has not yet been adjudicated, precedence for maintaining privacy through such torts exists (Thomson, 1975). Continued use of this method of job screening would likely increase public and private actions by social media users who might pressure social media companies to defend this contract through tort law. Furthermore, there are legal concerns related to the type of information that is available via social media and how one can use it. Social media provides much information (e.g., participants' race, ethnicity, age, gender, national origin, religion, disability status, pregnancy status, political affiliation, or union membership) that hiring managers can use to illegally discriminate against applicants (Kluemper & Rosen, 2009; Slovensky & Ross, 2012). Finally, there are legal concerns related to how organizations treat applicants if they honestly do not have a social media account. Although decreasing, a "digital divide" exists in the US in which some people do not have the same access to technology as others (Chou, Hunt, Beckjord, Moser, & Hesse, 2009). This divide raises concerns of disparate impact against some applicants if a hiring organization views one's not having a social media account negatively (Roth et al., 2013). Others might have ready access to social media but choose simply not to engage in the activity. We need future research to explore potential organizational and job applicant reactions to such activities.

As a final consideration for industry, some organizations might wish to create or purchase HRIS that attempt to automate the retrieval of job applicants' information found on publically accessible social media outlets after receiving a formal application in their information system. While such capability would make the vetting process much more efficient for organizations that use social media for hiring decisions, we warn that these organizations run the risk of having a decreased applicant pool altogether as individuals who view the request for social media credentials an unethical would likely simply not apply for the position. Thus, organizations could face backlash from their hiring process before the vetting process even commences.

6.3 Limitations

Because we examined an ethically questionable activity (i.e., HR requesting job applicants' social media login credentials), we could not directly test the condition without violating participants' privacy. We instead employed a scenario-based vignette, which is a common practice in business ethics research (Weber, 1992). This scenario, however, can only simulate unethical decision making intentions. We took steps to ensure the authenticity of the scenario by using an event that garnered sufficient public attention in the US. We also used a pilot study to ensure the scenario was plausible.

The vignette we used also limits the generalizability of the study somewhat. We specifically targeted a morally charged scenario, but that scenario is not common in practice. Future research should explore how other, more common job-screening techniques using social media data impacts job candidates' trust in the company and/or their privacy protective responses (Drake & Furner, 2015; Wang, Sun, Drake, & Hall, 2015). For example, future research could experimentally manipulate the morality of the issues by making them more or less salient in the immediacy, social consensus, or potential magnitude of harm. Such findings might help companies develop policies that best respect the privacy of job applicants while providing HR representatives with tools to screen candidates successfully.

Because our sample comprised undergraduate and graduate students, our findings are most germane to younger individuals. This limitation is important since research suggests that older individuals have different perceptions about privacy than younger individuals (Rainie, 2016). Accordingly, future research should include samples containing greater variance in participant age to increase generalizability.

Finally, when using a single method for collecting data, one always has to worry about common method bias in the results. While we used two common tests to assess common method bias in our survey data, they have their limitations (Podsakoff et al., 2003). Future research could expand on our study by using alternative methods of data collection or measuring data at different points in time. These alterations would help increase the generalizability of our findings. Furthermore, the order of the measurement items may have primed participants to answer survey questions in a particular way. Feldman and Lynch (1988) suggest that one can potentially mitigate priming in the order of questions by using a context that is personally relevant. We designed our vignette to be personally relevant to our participants: we used a

topic they were likely familiar with, used a context with a likely high affective reaction, and asked participants to imagine they were involved in the request. We also adapted the measurement items from existing measures. However, further research could help confirm our findings through extensive interviews and behavioral observation, experimental methods to infer inputs dominant in the absence of prior questioning, field experiments that asses the degree to which question placement influences reliability and validity, and the measurement of different subgroups of the population in susceptibility to measurement effects (Feldman & Lynch, 1988).

7 Conclusion

With this research, we discovered that individual ethical decisions and the perceived intensity of the moral dilemma increase job seekers' intentions to protect the information privacy of their social media accounts when confronted with requests for login credentials from potential employers. We explored six different information privacy protection responses and found that ethical judgments increased intentions to refuse to disclose, remove information, spread negative word-of-mouth, complain to company executives, and complain to third parties. Furthermore, we found that the perceived intensity of harmful consequences to the job applicant increased intentions to refuse to disclose, misrepresent themselves, remove information, complain to company executives, and complain to third parties. These findings add to the small but growing research stream in job screening with social media.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*, 509-514.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole Publishing.

Anderson, N. R. (2003). Applicant and recruiter reactions to new technology in selection: A critical review and agenda for future research. *International Journal of Selection and Assessment, 11*(2-3), 121-136.

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior, 38*(1), 33-42.

Barnett, T. (2001). Dimensions of moral intensity and ethical decision making: An empirical study. *Journal of Applied Social Psychology, 31*(5), 1038-1057.

Bata, N. A. (2009). Twelfph annual ADP screening index reveals nearly 10 percent of job candidates have criminal history, credit issues or driving citations. *ADP.* Retrieved from http://www.adp.com/media/press-releases/archive/2009-news-releases/twelfth-annual-adp-screening-index.aspx

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

Black, S. L., Stone, D. L., & Johnson, A. F. (2015). Use of social networking websites on applicants' privacy. *Employee Responsibility and Rights Journal, 27*(2), 115-159.

Brown, B. K., & Campion, M. A. (1994). Biodata phenomenology: recruiters' perceptions and use of biographical information in resume screening. *Journal of Applied Psychology, 79*(6), 897-908.

Brown, V. R., & Vaughn, E. D. (2011). The writing on the (Facebook) wall: the use of social networking sites in hiring decisions. *Journal of Business Psychology, 26*(1), 219-225.

Butterfield, K. D., Trevino, L. K., & Weaver, G. R. W. (2000). Moral awareness in business organizations: Influences of issue-related and social context factors. *Human Relations, 53*(7), 981-1018.

Cable, D. M., & Gilovich, T. (1998). Looked over or overlooked? Prescreening decisions and postinterview evaluations. *Journal of Applied Psychology, 83*(3), 501-508.

Chin, W. W. (2010). How to write up and report PLS analyses. In V. E. Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of partial least squares*. New York, NY: Springer Berlin Heidelberg.

Chou, W.-y. S., Hunt, Y. M., Beckjord, E. B., Moser, R. P., & Hesse, B. W. (2009). Social media use in the United States: Implications for health communication. *Journal of Medical Internet Research, 11*(4).

Cialdini, R. B. (2001). *Influence: Science and practice*. Boston: Allyn & Bacon.

Clark, L. A., & Roberts, S. J. (2010). Employer's use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics, 95*(4), 507-525.

Cole, J. I. (2011). The digital future project: Surveying the digital future year ten. *Center for the Digital Future.* Retrieved from http://www.digitalcenter.org/wp-content/uploads/2012/12/2011_digital_future_report-year10.pdf

Cole, M. S., Feild, H. S., & Giles, W. F. (2003). Using recruiter assessments of applicants' resume content to predict applicant mental ability and big five personality dimensions. *International Journal of Selection and Assessment, 11*(1), 78-88.

Cole, M. S., Feild, H. S., Giles, W. F., & Harris, S. G. (2009). Recruiters' inference of applicant personality based on resume screening: Do paper people have a personality? *Journal of Business and Psychology, 24*(1), 5-18.

Cole, M. S., Rubin, R. S., Feild, H. S., & Giles, W. F. (2007). Recruiters' perceptions and use of applicant résumé information: Screening the recent graduate. *Applied Psychology, 56*(2), 319-343.

Collins, C. J., & Stevens, C. K. (2002). The relationship between early recruitment-related activities and the application decisions of new labor-market entrants: A brand equity approach to recruitment. *Journal of Applied Psychology, 87*(6), 1121-1133.

Corcoran, S., Elliot, N., Bernoff, J., Pflaum, C. N., & Bowen, E. (2009). The broad reach of social technologies. *Forrester.* Retrieved from https://www.forrester.com/The+Broad+Reach+Of+Social+Technologies/fulltext/-/E-RES55132?docid=55132

Davis, D. C. (2007). MySpace isn't your space: Expanding the fair credit reporting act to ensure accountability and fairness in employer searches of online social networking services. *Kansas Journal of Law & Public Policy, XVI*(2).

Davison, H. K., Maraist, C., & Bing, M. N. (2011). Friend or foe? The promise and pitfalls of using social networking sites for HR decisions. *Journal of Business and Psychology, 26*(2), 153-159.

Deschenaux, J. (2015). State laws ban access to workers' social media accounts. Retrieved from http://www.shrm.org/legalissues/stateandlocalresources/pages/states-social-media.aspx

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.

Drake, J. R. (2016). Asking for Facebook logins: An egoist case for privacy. *Journal of Business Ethics*, *139*(3), 429-441.

Drake, J. R., & Furner, C. P. (2015). *Screening job candidates with social media: A manipulation of disclosure requests.* Paper presented at the 21st Americas Conference on Information Systems, Puerto Rico.

Drake, J. R., Hall, D., Cegielski, C., & Byrd, T. A. (2015). An exploratory look at early online auction decisions: Extending signal theory. *Journal of Theoretical and Applied Electronic Commerce Research, 10*(1), 35-48.

Drake, J. R., Hall, D. J., & Lang, T. (2009). *Ethical perspectives of business students: Development of a new instrument.* Paper presented at the Decision Sciences Institute 40th Annual Meeting.

Drouin, M., O'Connor, K. W., Schmidt, G. B., & Miller, D. A. (2015). Facebook fired: Legal perspectives and young adults' opinions on the use of social media in hiring and firing decisions. *Computers in Human Behavior, 46*(1), 123-128.

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). Social media update 2014. *PewResearchCenter.* Retrieved from http://www.pewinternet.org/2015/01/09/social-media-update-2014/

Efrati, A., & Lublin, J. S. (2012). Thompson resigns as CEO of Yahoo. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052702304192704577402224129006022

eMarketer (2013). Social networking reaches nearly one in four around the world. *eMarketer*. Retrieved from https://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976

Evans, J. B. T. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. *Annual Review of Psychology, 59*, 255-278.

Facebook. (2012). *Statement of rights and responsibilities*. Retrieved from https://www.facebook.com/legal/terms

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451-474.

Feldman, J. M., & Lynch, J. G. (1988). Self-generated validity and other effects on measurement on belief, attitude, intention, and behavior. *Journal of Applied Psychology, 73*(3), 421-435.

Fornell, C., & Larcker, D. F. (1981). Evaluting structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the AIS, 16*, 91-109.

Goe, L. C., Herrera, A. M., & Mower, W. R. (1998). Misrepresentation of research citations among medical school faculty applicants. *Academic Medicine, 73*(11), 1183-1186.

Grasz, J. (2009). Forty-five percent of employers use social networking sites to research job candidates, Careerbuilder survey finds. *Careerbuilder.* Retrieved from http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2F19%2F2009&ed=12%2F31%2F2009

Guillory, J., & Hancock, J. T. (2012). The effect of LinkedIn on deception in resumes. *Cyberpsychology, Behavior, and Social Networking, 15*(3), 135-140.

Jiang, Z., Heng, C. S., & Choi, B. C. F. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research, 24*(3), 579-595.

Jobvite (2015), Social recruiting survey results 2014. *Jobvite.* Retrieved from https://www.jobvite.com/wp-content/uploads/2014/10/Jobvite_SocialRecruiting_Survey2014.pdf

Jones, L. (1984). Lies, damned lies, and CVs. *Education + Training, 26*(4), 124-126.

Jones, T. M. (1991). Ethical decision making by individuals in organizations: An issue-contingent model. *Academy of Management Review, 16*(2), 366-395.

Kasper, K. (2015). Jobvite infographic: Watch what you post on social media. *Jobvite.* Retrieved from http://www.jobvite.com/blog/jobvite-infographic-watch-post-social-media/

Keith, M. J., Babb, J. S. J., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637-667.

Kluemper, D. H., & Rosen, P. A. (2009). Future employment selection methods: Evaluating social networking web. *Journal of Managerial Psychology, 24*(6), 567-580.

Kluemper, D. H., Rosen, P. A., & Mossholder, K. W. (2012). Social networking websites, personality ratings, and the organizational context: More than meets the eye? *Journal of Applied Social Psychology, 42*(5), 1143-1172.

Kuhn, K. M., Johnson, T. R., & Miller, D. (2013). Applicant desirability influences reactions to discovered resume embellishments. *International Journal of Selection and Assessment, 21*(1), 111-120.

Lehnert, K., Park, Y.-h., & Singh, N. (2014). Research note and review of the empirical ethical decision-making literature: Boundary conditions and extensions. *Journal of Business Ethics*, *129*(1), 195-219

Loch, K. D., & Conger, S. (1996). Evaluating ethical decision making and computer use. *Communication of ACM, 39*(7), 74-83.

Loe, T. W., Ferrell, L., & Mansfield, P. (2000). A review of empirical studies assessing ethical decision making in business. *Journal of Business Ethics, 25*(3), 185-204.

Lowry, P. B., Cao, J., & 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), 163-120.

Lucero, M. A., Allen, R. E., & Elzweig, B. (2013). Managing employee social networking: Evolving views from the national labor relations board. *Employee Responsibility and Rights Journal, 25*(3), 143-158.

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin, 18*(1), 3-9.

Malhotra, N. K., Kim, S. S., & Agarwal, R. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), p. 5 - 12.

May, D. R., & Pauli, K. P. (2002). The role of moral intensity in ethical decision-making: A review and investigation of moral recognition, evaluation, and intention. *Business & Society, 43*(1), 84-117.

McDonald, G., & Pak, P. (1996). It's all fair in love, war, and business: Cognitive philosophies in ethical decision making. *Journal of Business Ethics, 15*, 973–996.

Mikula, G., Scherer, K. R., & Athenstaedt, U. (1998). The role of injustice in the elicitation of differential emotional reactions. *Personality and Social Psychology Bulletin, 24*(7), 769-783.

Miner, M., & Petocz, A. (2003). Moral theory in ethical decision making: Problems, clarifications and recommendations from a psychological perspective. *Journal of Business Ethics, 42*(1), 11-25.

Mizutami, M., Dorsey, J., & Moor, J. H. (2004). The Internet and Japanese conception of privacy. *Ethics and Information Technology, 6*(2), 121-128.

Moore, A. (2010). *Privacy rights: Moral and legal foundations*. University Park, PA: The Pennsylvania State Universiy Press.

O'Dell, J. (2012). Recruitment trend we hate: Asking for Facebook passwords during the interview. *Venturebeat.* Retrieved from http://venturebeat.com/2012/03/21/facebook-login-job-interview/

O'Fallon, M. J., & Butterfield, K. D. (2005). A review of the empirical ethical decision-making literature: 1996-2003. *Journal of Business Ethics, 59*(4), 375-413.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principle-agent perspective. *MIS Quarterly, 31*(1), 105-136.

Peikoff, A. (2008). Beyond reductionism: Reconsidering the right to privacy. *NYU Journal of of Law & Liberty, 3*(1), 1-47.

Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure.* Albany: State University of New York Press.

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

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems, 19*(2), 181-195.

Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs, 4*(4), 323-333.

Rainie, L. (2016). The state of privacy in post-Snowden America. *PewResearchCenter*. Retrieved from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

Reidenbach, R., & Robin, D. (1990). Toward the development of a multidimensional scale for improving evaluations of business ethics. *Journal of Business Ethics, 9*(8), 639-653.

Resnick, P., Zeckhauser, R., Friedman, E., & Kuwabara, K. (2000). Reputation systems. *Communications of the ACM, 43*(12), 45 - 48.

Rest, J. R. (1986). *Moral development: Advances in research and theory*. New York: Praeger.

Rest, J. R., Narvaez, D., Bebeau, M. J., & Thoma, S. J. (1999). *Postconventional moral thinking: A neo-Kohlbergian approach*. Mahwah, NJ: Lawrence Erlbaum.

Reynolds, S. J. (2006). Moral awareness and ethical predispositions: Investigating the role of individual differences in the recognition of moral issues. *Journal of Applied Psychology, 91*(1), 233-243.

Roth, P. L., Bobko, P., Van Iddenkinge, C. H., & Thatcher, J. B. (2013). Social media in employee-selection-related decisions: A research agenda for uncharted territory. *Journal of Management*.

Rozelle, A. L., & Landis, R. S. (2002). An examination of the relationship between use of the Internet as a recruitment source and student attitudes. *Computers in Human Behavior, 18*(5), 593-604.

Ruegger, D., & King, E. W. (1992). A study of the effect of age and gender upon student business ethics. *Journal of Business Ethics, 11*(3), 179-186.

Schmidt, G. B., & O'Connor, K. W. (2015). Fired for Facebook: Using NLRB guidance to craft appropriate social media policies. *Business Horizons, 58*(5), 571-579.

Schwartz, P. (1989). On moral sanctions. *The Intellectual Activist, 5*(1), 7-8.

Siebert, S., Downes, P. E., & Christopher, J. (2012). *Applicant reactions to online background checks: Welcome to a brave new world.* Paper presented at the Academy of Management.

Singhapakdi, A., Vitell, S. J., & Kraft, K. L. (1996). Moral intensity and ethical decision-making of marketing professionals. *Journal of Business Research, 36*(3), 245-255.

Slovensky, R., & Ross, W. H. (2012). Should human resource managers use social media to screen job applicants? Managerial and legal issues in the USA. *Info, 14*(1), 55-69.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1015.

Smith, J. (2012). Make social media your job-finding weapon. *Forbes.* Retrieved from http://www.forbes.com/sites/jacquelynsmith/2012/04/20/make-social-media-your-job-finding-weapon/

Smith, T. (2000). *Viable values: A study of life as the root and reward of morality*. Lanham, MD: Rowman & Littlefield Publishers.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32*(3), 503-529.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36-49.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. In G. R. Ferris & K. M. Rowland (Eds.), *Research in personnel and human resources management* (vol. 8, pp. 349-411). Greenwich, CT: JAI Press.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*(1), 590-598.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1-22.

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *Computers and Society, 31*(1), 6-11.

Thomson, J. J. (1975). The right to privacy. *Philosophy and Public Affairs, 4*(4), 295-314.

Trevino, L. K. (1986). Ethical decision making in organizations: A person-situation interactionist model. *Academy of Management Review, 11*(3), 601 - 617.

Valentine, S., & Fleischman, G. (2006). Ethical reasoning in an equitable relief innocent spouse context. *Journal of Business Ethics, 45*(4), 325-339.

Van Hoye, G., & Lievens, F. (2005). Recruitment-related information sources and organizational attractiveness: Can something be done about negative publicity? *International Journal of Selection and Assessment, 13*(3), 179-187.

Van Hoye, G., & Lievens, F. (2007). Social influences on organizational attractiveness: Investigating if and when word-of-mouth matters. *Journal of Applied Social Psychology, 37*(9), 2024-2047.

Van Hoye, G., & Lievens, F. (2009). Tapping the grapevine: A closer look at word-of-mouth as a recruitment source. *Journal of Applied Psychology, 94*(2), 341-352.

van Iddenkinge, C. H., Lanivich, S. H., Roth, P. L., & Junco, E. (2013). Social media for selection? Validity and adverse impact potential of a Facebook-based assessment. *Journal of Management*.

Wang, Y., Sun, S., Drake, J. R., & Hall, D. (2015). *Job applicants' information privacy-protective response: Exploring the roles of technology readiness and trust.* Paper presented at the 21st Americas Conference on Information Systems.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Watley, L. D., & May, D. R. (2004). Enhancing moral intensity: The role of personal and consequential information in ethical decision-Making. *Journal of Business Ethics, 50*(2), 105-126.

Weber, J. (1992). Scenarios in business ethics research: review, critical assessment, and recommendations. *Business Ethics Quarterly, 2*(2), 137-160.

Wetzer, I. M., Zeelenberg, M., & Pieters, R. (2007). "Never eat in that restaurant, i did!": Exploring why people engage in negative word-of-mouth communication. *Psychology & Marketing, 24*(8), 661-680.

Woiceshyn, J. (2011). A model for ethical decision making in business: Reasoning, intuition, and rational moral principles. *Journal of Business Ethics, 104*(3), 311-323.

Zhang, P., & Li, N. (2005). The intellectual development of human-computer interaction research: A critical assessment of the MIS literature (1990-2002). *Journal of the Association for Information Systems, 6*(11), 227-292.

Appendix A: Questionnaire

Concern for information privacy (Stewart & Segars, 2002)

Please specify the extent to which you agree or disagree with the following statements:

1. It usually bothers me when companies ask me for personal information.
2. When companies ask me for personal information, I sometimes think twice before providing it.
3. It bothers me to give personal information to so many people.
4. I am concerned that companies are collecting too much personal information about me.

Recognize moral issue (Reynolds, 2006)

Please specify the extent to which you agree or disagree with the following statements:

1. There are very important ethical concerns with the interviewer's request to provide usernames and passwords.
2. The interviewer's request to provide usernames and passwords clearly involves moral issues.

Make judgment

Please specify the extent to which you agree or disagree with the following statements:

1. The interviewer's request to provide usernames and passwords make me uncomfortable.
2. It is clearly immoral for the organization to make this request for usernames and passwords.
3. It is wrong for the interviewer to make this request.

Moral intensity (Barnett, 2001)

Social consensus: please indicate the extent you believe society as a whole considers the interviewer's request to provide usernames and passwords to be…

1. Unethical-ethical
2. Wrong-right
3. Inappropriate-appropriate

Temporal immediacy: negative consequences to me as a result of sharing my usernames and passwords are going to occur

1. After a long time-immediately
2. Slowly-quickly
3. Gradually-rapidly

Magnitude of consequence: please indicate the degree of harm from sharing usernames and passwords will be:

1. Minor-severe
2. Insignificant-significant
3. Slight harm-great harm

IPPR intention (Son & Kim, 2008)

Refusal: seven-point semantic scales

Please specify the extent to which you would refuse to give your username and password to the organization because you think it is too personal.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Misrepresentation: seven-point semantic scales

Please specify the extent to which you would falsify some of your personal information if you comply with the interviewer's request.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Removal: seven-point semantic scales

Please specify the extent to which you would take actions to have information removed from the social media platform if you comply with the interviewer's request.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Negative word-of-mouth: seven-point semantic scales

Please specify the extent to which you would speak to your friends and/or relatives about the interviewer's request.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Complaining directly to company executives: seven-point semantic scales

Please specify the extent to which you would write or call executives in this organization to complain about the interviewer's request.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Complaining indirectly to third-party organizations: seven-point semantic scales

Please specify the extent to which you would write or call an elected official, a news agency, or a business organization to complain about the request.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

About the Authors

John Drake is an Assistant Professor of Management Information Systems at East Carolina University. He holds a BS in Physics from Southern Illinois University at Edwardsville and a PhD in Management of Information Technology and Innovation from Auburn University. His research has been published in journals such as *Journal of Business Ethics, IEEE Transactions on Professional Communication, Journal of Information Technology Theory and Application, Journal of Theoretical and Applied Electronic Commerce Research,* and the *Journal of Information Technology Education*. His current research interests focus on developing effective web presence strategies, social media privacy, project management, online education, and business ethics. Prior to academia, he was an IT professional and consultant for 5 years.

Dianne Hall is a Torchmark Professor of Information Systems Management and Analytics at Auburn University. She holds a doctorate in Information and Operations Management from Texas A&M University. Her work appears in academic and practitioner journals such as the *Journal of the Association for Information Systems, Decision Support Systems, Communications of the Association for Information Systems, International Journal of Physical Distribution and Logistics Management, International Journal of Logistics Management, Communications of the Association for Computing Machinery*, and others. Her work has also appeared in several books. Her current research interests include applications of information technologies and analytics in support of knowledge management, logistics, supply chain resiliency, sustainability, and contingency planning, as well as enhanced decision making processes.

J. Bret Becton, PhD, is the Associate Dean for Operations and Accreditation and an Associate Professor of Management in the College of Business at Southern Miss. He received a B.S. degree in Psychology from the University of Southern Mississippi, a M.A. in Industrial-Organizational Psychology from the University of Tulsa, and a Ph.D. in Management from Auburn University. His research interests revolve around employee recruitment and staffing, employee turnover, organizational citizenship behavior and counterproductive work behavior and his research has been published in *Journal of Applied Psychology, Journal of Vocational Behavior, Journal of Organizational Behavior, Journal of Business & Psychology, Corporate Governance: An International Review, Business Horizons, International Journal of Selection and Assessment, International Journal of Human Resource Management, Journal of Applied Social Psychology,* and *Journal of Management & Organization*. Additionally, he has provided consulting services for clients such as the National Center for Spectator Sport Security (NCS4), Jackson County Utility Authority, Southern Farm Bureau Life Insurance Company, Equal Employment Opportunity Commission, Pine Belt Mental Healthcare Resources, and Steel Service Corporation.

Clay Posey is an associate professor of Management Information Systems in the Culverhouse College of Commerce and the associate director of the Cyber Institute at The University of Alabama. He received his DBA from Louisiana Tech University and has research interests in behavioral information security, online self-disclosure, and research methods among others. His research has been presented at various national and international conferences and has been published or is forthcoming in several academic journals including but not limited to *MIS Quarterly*, *Journal of Management Information Systems*, *European Journal of Information Systems, Information Systems Journal, Information & Management, The DATA BASE for Advances in Information Systems,* and *Computers & Security*. He is currently an associate editor for *Information & Management* and is a member of the IFIP Working Group 8.11/11.13 on Information Systems Security Research.

Transactions on Human – Computer Interaction